The Office of the National Coordinator for
Health Information Technology

Connecting Health and Care for the Nation

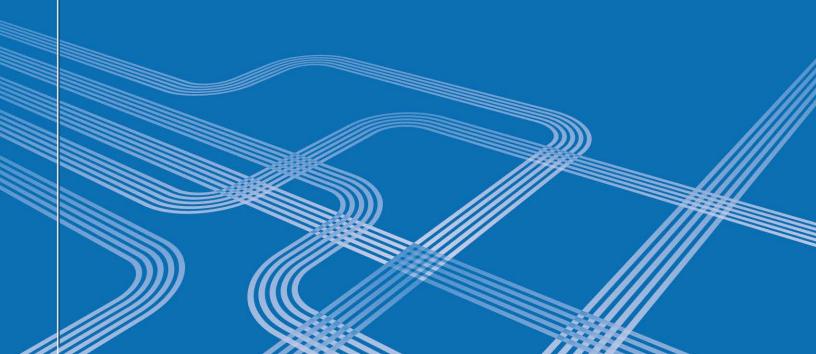A Shared Nationwide Interoperability Roadmap

DRAFT Version 1.0

Table of Contents

Letter from the National Coordinator

In June 2014, the Office of the National Coordinator for Health Information Technology (ONC) laid out a vision for a future health IT ecosystem where electronic health information is appropriately and readily available to empower consumers, support clinical decision-making, inform population and public health and value based payment, and advance science. In *Connecting Health and Care for the Nation*: A 10-Year Vision to Achieve an Interoperable Health IT Infrastructure (ONC's 10-Year Interoperability Concept Paper)[1]*, ONC committed* to leading and collaborating with the health IT and health sector to define a shared Roadmap for achieving interoperable health IT that supports a broad scale learning health system by 2024. This Roadmap reflects the result of that collaborative work with federal, state and private partners. It lays out a plan for what needs to happen, by when, and by whom, to see that electronic health information is available when and where it matters most for those we are here to serve: the American people.

In the decade since ONC began its service to the nation, the United States has experienced remarkable progress in the digitization of the health experience. There has also been significant advancement of payment reform that is driving the need for better visibility of the care experience and demand for straightforward quality measurement. Consumers are increasingly expecting their electronic health data to be available when and where it matters to them, just as their data is in other sectors. And new technology is allowing for a more accessible, affordable and innovative approach. However, barriers remain to the seamless sharing and use of electronic health information.

This draft Roadmap proposes critical actions that the public and private sector need to take to advance the country towards an interoperable health IT ecosystem over the next 10 years. Achieving such an interoperable system is an essential element towards HHS Secretary Sylvia Burwell's vision of better care through smarter spending, leading to healthier people. Achieving that better care system and better health for all will, through health IT interoperability, require work in 3 critical pathways: 1) Requiring standards; 2) Motivating the use of those standards through appropriate incentives; and 3) Creating a trusted environment for the collecting, sharing and using of electronic health information. It will require us to agree to a set of rules of engagement that will bring trust to the system for consumers and others, it will allow us to see that the privacy expectations of consumers are respected, that states are aligned in policy, that we are aligning payment and other levers to advance and sustain a durable interoperable ecosystem, to make data more portable and liquid with tools like APIs, and to have a set of standards that allow more seamless, yet appropriate, sharing of electronic health information for "small" (individual patient), "big" (population level and beyond) and "long" data (wrapping around the individual and telling their health story over time).

---

[1] http://www.healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf

We are thankful to our federal, state and private sector partners who have worked with us over these past few months to shape this path forward and help us to identify the most impactful actions to achieve a learning health system.   To date, there have been contributions from over forty individuals and organizations, twenty-five federal partners, 90 individuals from 38 states and ONC's Federal Advisory Committees (FACAs) whose membership includes 167 representatives from over 140 private and public organizations.

The Roadmap identifies critical actions that should be taken by a wide range of stakeholders to help advance nationwide interoperability. I invite you to review the Roadmap, provide your input and choose a critical action that you are willing to commit to, or even take the lead on. It is only through everyone's combined efforts that we will achieve a learning health system that brings real value to electronic health information as a means to better care, wiser spending, and healthier people.

This Roadmap is intended to be a living document owned and guided in its evolution by all health IT stakeholders.   Because the Office of the National Coordinator for Health IT (ONC) is charged with supporting the adoption of health IT and promoting nationwide health information exchange to improve health and care, it has played a major role in coordinating with a broad array of stakeholders to develop this initial draft. ONC will continue to support stakeholders by coordinating input and publishing future versions of the Roadmap. ONC is accepting public comment on this draft version of the Roadmap until 5 p.m. ET on April 3, 2015 on www.healthit.gov/interoperability. After carefully reviewing and integrating the public's feedback, ONC will release an updated Roadmap later in 2015.

ONC is also releasing an open draft of the 2015 Interoperability Standards Advisory that is an initial version of a "best available standards and implementation specifications" list for interoperability of clinical health information that enables priority learning health system functions [2]. Development of this list is identified as a critical action in the Roadmap that ONC has committed to. Please review this list and provide comments on www.healthit.gov/interoperability. While you take time out to comment on these documents, please do not slow your work to advance interoperability.

Thank you for your participation in this collaborative process. And thank you in advance for your thoughtful comments and willingness to take the lead on critical actions. It is a testament to the remarkable spirit of this nation's health IT community and our shared interest in putting the person at the center.

Karen B. DeSalvo, MD, MPH, MSc
National Coordinator for Health Information Technology

---

[2] The scope of the Advisory is on clinical health information exchange, and does not reference standards related to HIPAA transactions. The priority learning health functions are the business and technical requirements for a Learning Health System that are in the Roadmap introduction.

Questions on the Roadmap

As you review the Roadmap, please consider the following questions and submit your responses during the public comment period.

1. **General**
   1. Are the actions proposed in the draft interoperability Roadmap the right actions to improve interoperability nationwide in the near term while working toward a learning health system in the long term?
   2. What, if any, gaps need to be addressed?
   3. Is the timing of specific actions appropriate?
   4. Are the right actors/stakeholders associated with critical actions?

2. **Priority Use Cases**
   1. Appendix H lists the priority use cases submitted to ONC through public comment, listening sessions, and federal agency discussions. The list is too lengthy and needs further prioritization. *Please submit 3 priority use cases from this list that should inform priorities for the development of technical standards, policies and implementation specifications.*

3. **Governance**
   1. The draft interoperability roadmap includes a call to action for health IT stakeholders to come together to establish a coordinated governance process for nationwide interoperability. ONC would like to recognize and support this process once it is established. How can ONC best recognize and support the industry-led governance effort?

4. **Supportive Business, Cultural, Clinical and Regulatory**
   1. How can private health plans and purchasers support providers to send, find or receive common clinical data across the care continuum through financial incentives? Should they align with federal policies that reinforce adoption of standards and certification?

5. **Privacy and Security Protections for Health Information**
   1. What security aspects of RESTful services need to be addressed in a standardized manner?

6. **Core Technical Standards and Functions**
   1. Which data elements in the proposed common clinical data set list need to be further standardized? And in what way?
   2. Do you believe the approach proposed for Accurate Individual Data Matching will sufficiently address the industry needs and address current barriers?

7. **Certification and Testing**
   1. In what ways can semantic interoperability be best tested? (e.g., C-CDA content and semantics)

8. **Measurement**
    1. 1. Does the measurement and evaluation framework cover key areas? What concepts are missing?
    2. Which concepts from the framework are the most important to measure? What types of measures should be included in a "core" measure set?
    3. Should measurement focus on certain use cases, priority populations or at certain levels of the ecosystem (e.g., encounter, patient, provider, organization)?
    4. What other types of metrics have been successfully used at the local or regional level that might be considered for nationwide use? Would stakeholders be willing to propose novel metrics and provide "test beds" to assess the potential for nationwide use?
    5. What measurement gaps should be prioritized and addressed quickly?
    6. What other available data sources at the national level could be leveraged to monitor progress?
    7. Are the potential mechanisms for addressing gaps adequate? What are other suggestions?
    8. How should data holders share information to support reporting on nationwide progress?
    9. What are appropriate, even if imperfect, sources of data for measuring impact in the short term? In the long term? Is there adequate data presently to start some measurement of impact?

Executive Summary

Introduction

Health information technology (health IT) that facilitates the secure, efficient and effective sharing and use of electronic health information when and where it is needed is an important contributor to improving health outcomes, improving health care quality and lowering health care costs – the three overarching aims that the U.S. is striving to achieve. Health IT can help health care providers recommend treatments that are better tailored to an individual's preferences, genetics and concurrent treatments; it can help individuals make better treatment decisions and health-impacting decisions outside of the care delivery system; and can help reduce care delivery redundancy and cost by allowing test results to be reused while supporting analyses to pinpoint waste. To achieve this, however, the health IT community must expand its focus beyond institutional care delivery and health care providers, to a broad view of person-centered health. This shift is critical for at least two reasons:

1. Health care is being transformed to deliver care and services in a person-centered manner and is increasingly provided through community and home-based services that are less costly and more convenient for individuals and caregivers; and
2. Most determinants of health status are social and are influenced by actions and encounters that occur outside traditional institutional health care delivery settings, such as in employment, retail, education and other settings.

This shift requires a high degree of information sharing between individuals, providers and organizations and therefore a high degree of interoperability between many different types of health IT, such that systems can exchange and use electronic health information without special effort on the part of the user.[3] The goal of this shift is to a nationwide learning health system—an environment that links the care delivery system with communities and societal supports in "closed loops" of electronic health information flow, at many different levels, to enable continuous learning and improved health. This kind of system allows individuals to select platforms and apps to share and use their own electronic health information to meet their needs without undue constraints.

This shared nationwide interoperability Roadmap describes the actions and roles of a variety of health IT stakeholders needed to achieve the vision described in ONC's 10-Year Interoperability Concept Paper[4]. This 10-year Roadmap describes barriers to interoperability across the current health IT landscape, the desired future state that the industry believes will be necessary to enable a learning health system and a suggested path for moving from the current state to the desired future state. The Roadmap lays out a path to achieving the vision in the three-, six- and ten-year time frames and a vision to catalyze

---

[3] Derived from the Institute of Electrical and Electronics Engineers (IEEE) definition of interoperability.

[4] http://www.healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf

collaboration and action across government, communities and the private sector. As such, the Roadmap will enable stakeholders to make key commitments and take actions that align with other stakeholder actions, in order for the nation to collectively move towards a learning health system.

Principle-Based Interoperability: Working Toward a Long-Term Vision with Near-Term Wins

An interoperable health IT ecosystem that is person-centered makes the right electronic health information available to the right people at the right time across products and organizations, in a way that can be relied upon and meaningfully used by recipients. This ecosystem should adhere to the following interoperability guiding principles (Figure 1).

Figure 1: Principles of Interoperability

BUILD UPON EXISTING HEALTH IT INFRASTRUCTURE	MAINTAIN MODULARITY	ONE SIZE DOES NOT FIT ALL
CONSIDER THE CURRENT ENVIRONMENT AND SUPPORT MULTIPLE LEVELS OF ADVANCEMENT	EMPOWER INDIVIDUALS	SIMPLIFY
PROTECT PRIVACY AND SECURITY IN ALL ASPECTS OF INTEROPERABILITY	LEVERAGE THE MARKET	FOCUS ON VALUE
	SCALABILITY AND UNIVERSAL ACCESS	

Based on these principles, this *Shared Nationwide Interoperability Roadmap* identifies functional and business requirements for interoperability and lays out a foundational set of short-term and long-term critical actions for all stakeholders to work towards over the next 10 years in support of a learning health system. This vision significantly expands the types of information, information sources and information users well beyond clinical information derived from electronic health records (EHRs).

Specifically, the Roadmap focuses on actions that will enable a majority of individuals and providers across the care continuum to send, receive, find and use a common set of electronic clinical information at the nationwide level by the end of 2017. Although this near-term target focuses on individuals and care providers, interoperability of this core set of electronic health information will also be useful to community-based services, social services, public health and the research community. This includes standardized data elements, such as demographics, that will enable better matching and linking of electronic health information across all systems and platforms.

These standardized data elements support better stratification of electronic health information when aggregated to identify and address important issues such as health disparities and also support research and evidence-based personalized medicine. The intersection of clinical and administrative electronic health information is a critical consideration, but is out of scope for the Roadmap at this particular time. Use cases, standards, technologies and tools that leverage both administrative and clinical electronic health information will be an important topic to address in future iterations. There are also many aspects of health IT beyond interoperability that are important and will be critical to a learning health system, including technology adoption,[5] data quality, usability and workflow. However, these topics are out of scope for this Roadmap at this particular time and deserve separate, dedicated attention.

Given the increasing volume of mobile technology usage among consumers and across the care delivery system, approaches to enable "send, receive, find and use" in the near-term must support the flow of electronic health information across both institutional and mobile-based technologies. This means traditional approaches to health IT interoperability will need to become more agile and leverage the experience of modular consumer applications, such as those created by Facebook, Amazon and Apple. These secure, but simple architectures have enabled an ecosystem of applications that allow users to engage with electronic health information across a variety of different platforms and devices and open opportunities for entrepreneurial third parties to thrive.

Current Context

Many successful electronic health information-sharing arrangements currently exist in communities across the nation. These arrangements have often formed around specific geographies, networks and/or technology developers. However, several barriers continue to inhibit nationwide interoperability despite these arrangements and must be overcome rapidly to achieve a learning health system. These barriers include:

1. Electronic health information is not sufficiently structured or standardized and as a result is not fully computable when it is accessed or received. That is, a receiver's system cannot entirely process, parse and/or present data for the user in meaningful and useable ways. It is also difficult for users to know the origin (provenance) of electronic health information received from external sources. Workflow difficulties also exist in automating the presentation of

---

[5] Federal Health IT Strategic Plan 2015-2020 Goal One.

externally derived electronic health information in meaningful and appropriately non-disruptive ways.

2. Even when technology allows electronic health information to be shared across geographic, organizational and health IT developer boundaries, a lack of financial motives, misinterpretation of existing laws governing health information sharing and differences in relevant statutes, regulations and organizational policies often inhibit electronic health information sharing.

3. While existing electronic health information sharing arrangements and networks often enable interoperability across a select set of participants, there is no reliable and systematic method to establish and scale trust across disparate networks nationwide according to individual preferences.

A variety of electronic health information sharing arrangements and networks will continue to exist for the foreseeable future, as these arrangements serve important market and clinical functions by meeting the unique needs of many different communities. In a country as large and heterogeneous as the U.S., it is not realistic to suggest that all health information needs will be met with a single electronic health information sharing approach. However, the health IT ecosystem must evolve to address each of these barriers in a lasting and meaningful way to achieve a learning health system that protects the health of all Americans and provides essential human services to all.

While each electronic health information sharing arrangement may continue to use its own policies, service agreements and technical standards to support participant priorities and needs, a common set of policies and technical standards must be adopted across the ecosystem to support nationwide interoperability and transcend these disparate networks. This will provide electronic health information users the flexibility to use services with deep local electronic health information sharing functions that meet many of their day-to-day needs, while having the confidence that they can still engage in key universal transactions with any authorized users in any network.

This approach is consistent with the way the Internet operates today and with the interoperability trajectory experienced in other industries, such as telephone and ATM networks. Such market-based network development is critical to the achievement of nationwide interoperability. HHS will consider where additional guidance may be needed to clarify the current legal framework, including Health Insurance Portability and Accountability Act (HIPAA) Rules, to effectively support individual privacy in a learning health system.

Critical Actions for Near Term Wins

The four most important actions for public and private sector stakeholders to take to enable nationwide interoperability of electronic health information through health IT in the near term are: (1) establish a coordinated governance framework and process for nationwide health IT interoperability; (2) improve technical standards and implementation guidance for sharing and using a common clinical data set; (3) enhance incentives for sharing electronic health information according to common technical standards, starting with a common clinical data set; and (4) clarify privacy and security requirements that enable interoperability. Additional actions are needed in several other areas such as clinical culture, state and

organization-level policies; these actions are described in greater detail throughout the Roadmap. However, these four foundational actions are linchpins to achieving the near-term and long-term goals described in *Connecting Health a*nd *Care for the Nation* (Figure 2)*.* Below are more detailed near-term actions for each of these high priority areas.

1. *Establish a coordinated governance framework and process for nationwide health information interoperability.* As described above, the proliferation of health information sharing arrangements has created many different processes and rules for interoperability among sub-components of the health IT ecosystem. To enable nationwide interoperability for a common clinical data set, there must be agreement on the policies, operations and technical standards that will enable trust and allow information to be shared appropriately across the ecosystem. To that end, ONC will ensure the establishment of (1) a governance framework with overarching rules of the road for interoperability of health IT, (2) a public/private process for addressing implementation or operational-level issues and (3) a method for recognizing the organizations that comply with the rules and hold them accountable for continuing to do so. Public and private stakeholders will need to come together through a coordinated governance process to establish more detailed policies regarding business practices (including policies for identifying and addressing bad actors) and to identify the technical standards that will enable interoperability for specific use cases. See the Governance functional requirement for more detail on coordinated governance.

2. *Improve technical standards and implementation guidance for sharing and using a common clinical data set.* This basic set of electronic health information must be accessible via clinical documents (for example, in a care summary) and as discrete data elements (for example to plot blood pressure over time). It is unlikely that the care delivery system will stop using clinical documents for specific purposes in the near term (or perhaps the long term) and mobile technologies and applications will need to simultaneously access specific data elements to support individuals in the near term. The purpose for which electronic health information is shared and used must drive the technical standards and methods selected for nationwide adoption through a coordinated governance process. While coordinated governance processes are established, public and private stakeholders should advance standards that are scalable, high performing and

A Common Clinical Data Set
▸ Patient name
▸ Sex
▸ Date of birth
▸ Race
▸ Ethnicity
▸ Preferred language
▸ Smoking status
▸ Problems
▸ Medications
▸ Medication allergies
▸ Laboratory test(s)
▸ Laboratory value(s)/result(s)
▸ Vital signs
▸ Care plan field(s), including goals and instructions
▸ Procedures
▸ Care team members
▸ Immunizations
▸ Unique device identifier(s) for a patient's implantable device(s)
▸ Notes/narrative

simple. These standards should enable sharing a common clinical data set[6], further constrain implementations of the C-CDA and define standards for data provenance at the document and data element levels and implement standards in a manner that makes sharing and receiving electronic health information easy for users. See the Core Technical Standards and Functions building block for more detail on technical standards actions.

3. *Advance incentives for sharing health information according to common technical standards, starting with a common clinical data set.* While the Medicare and Medicaid EHR Incentive Programs (EHR Incentive Programs) have been a primary motivator for the adoption and use of health IT, these programs alone are insufficient to create economic incentives that lead to interoperability across the care continuum and, over time, a learning health system. Experience has demonstrated that current fee-for-service payment policies often deter the exchange of electronic health information, even when it is technically feasible. To ensure that individuals and providers can send, receive, find and use a common clinical data set, federal, state and commercial payers will need to evolve policy and funding levers. These levers should incentivize information sharing according to technical standards designated through ONC's HIT Certification Program in the near term and standards identified through the coordinated governance process over the longer term. See the Supportive Business and Regulatory Environment that Encourages Interoperability requirement for more detail on payment policy actions.

4. *Clarify privacy and security requirements that enable interoperability*. While health IT developers can design health IT tools that support electronic health information sharing, it is important to remember that the majority of clinical information resides within and is stewarded by health care organizations. Many of these health care organizations are "covered entities" (CEs) and are governed by the HIPAA Privacy and Security Rules. In addition, "business associates" (BAs) must follow parts of the HIPAA Privacy Rule and all of the requirements in the HIPAA Security Rule. Generally, BAs are organizations that perform certain functions or services to CEs that involve the use or disclosure of individually identifiable health information. The HIPAA Privacy Rule was designed to ensure that individuals' health information is protected while allowing the flow of health information needed to provide high quality health care. The HIPAA Security Rule was designed to protect the privacy of individuals' electronic health information while allowing the adoption of new technologies that will improve the quality and efficiency of patient care. Therefore, it is important for CEs and BAs to have consistent understanding of these requirements aligned with guidance provided by the HHS Office for Civil Rights.

---

[6] Vitals in particular should be expanded to include – patient's body height, body weight measured, diastolic and systolic blood pressure, heart rate, respiratory rate, body temperature, oxygen saturation in arterial blood by pulse oximetry, body mass index (ratio). Vitals should also include date and time of vital sign measurement or end time of vital sign measurement and the measuring- or authoring-type source of the vital sign measurement

Many organizations have misinterpreted HIPAA rules and other regulations and therefore refrain from sharing health information, even with individuals themselves. Effectively honoring the privacy and security of identifiable health information means that CEs and BAs will never be able to "open" or release identifiable health information writ large to whomever wishes to access it; however, in order to achieve nationwide interoperability, all organizations regulated by HIPAA must understand in the same way that HIPAA, through its permitted uses and its privacy protections, actually enables interoperability. With improved understanding, CEs and BAs will be able to exchange appropriately with greater confidence. This includes ensuring that individuals can exercise their legal right under HIPAA rules to access their own health information. Federal agencies and other stakeholders should work to provide the Office for Civil Rights, which enforces and issues guidance on the HIPAA Rules, with information it needs to determine whether additional guidance is needed to support interoperability while maintaining the crucial privacy protections on which interoperability relies. See the Privacy and Security Protections for Health Information building block for more detail on privacy and security actions.

See Figure 2 for a timeline of select high-level critical actions. These and other critical actions are described in detail throughout the Roadmap. The Roadmap is organization according to the following five fundamental building blocks.

- Core technical standards and functions
- Certification and testing to support adoption and optimization of health IT products and services
- Privacy and security protections for health information
- Supportive business, clinical, cultural and regulatory environments
- Rules of engagement and governance

Within each building block, the roadmap describes functional and business requirements for a learning health system and the associated actions for making rapid near term progress.

Figure 2: Timeline of Select High-Level Critical Actions for Near-Term Wins

| 2015 | 2016 | 2017 | 2018 | 2019 | 2020 |

Interoperability Roadmap: High-level Critical Actions for Near-term Wins

Existing communities agree on coordinated governance process

Coordinated governance process and single trust framework implemented

COORDINATED GOVERNANCE, EXCHANGE AND TRUST COMMUNITIES

Common rules of the road established

Coordinated governance process expands and maintains the common rules of the road

ONC to publish and annually update a list of the best available standards for interoperability

FHIR specs for querying a common clinical data set refined and piloted

Tech developers implement/FHIR spec for a common clinical data set

STANDARDS FOR INTEROPERABILITY

Data provenance specs published

Tech developers implement specs to support data provenance industry needs

C-CDA 2.0 released to public

Tech developers implement C-CDA implementation guidance

Tech developers roll out 2015 certified products

Clarify privacy and security requirements to enable interoperability

All public and private payers to evolve policy and funding levers

DRIVERS AND REGULATORY

★ 2015 ed. ONC Cert. & MU stage 3 NPRMs

★ 2015 ed. ONC Cert. & MU stage 3 FRs

★ MU stage 3 begins

Care providers across the continuum use 2014/2014 r.2 certified products/services

CARE PROVIDERS AND CONSUMER USE OF TECHNOLOGY

Consumers use online portals to access health info

Care providers across the continuum upgrade to 2015 certified products/services

Consumers aggregate health info from many portals in one place via apps

MILESTONES
Roadmap v 1.0 △

Target: Send, receive, find and use a common clinical data set to improve health and health care quality. △

Target: Expanded interoperable data and users to improve health and lower costs △

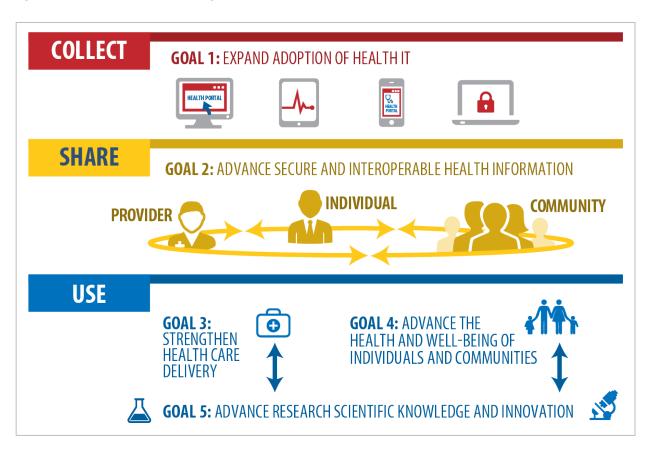Disclaimer: Timeframes noted are approximate estimates.

Roadmap Introduction

The Federal Health IT Strategic Plan

The draft Federal Health IT Strategic Plan 2015-2020 describes a set of overarching goals (see Figure 3) that align with HHS' aims of improving health care quality, lowering health care costs and improving the U.S. population's health.[7] This Nationwide Interoperability Roadmap describes a path for achieving the Strategic Plan's second goal (advance secure and interoperable health information) which helps the entire nation realize goals three, four and five through the development of a nationwide learning health system[8].

Figure 3: Federal Health IT Strategic Plan Goals

---

[7] See http://www.ahrq.gov/workingforquality/about.htm for more information on the National Quality Strategy
[8] Federal Health IT Strategic Plan 2015-2020. ONC. December 8, 2014.
http://www.healthit.gov/sites/default/files/federal-healthIT-strategic-plan-2014.pdf

Interoperability Vision for the Future

An interoperable health IT ecosystem makes the right data available to the right people at the right time among disparate products and organizations in a way that can be relied upon and meaningfully used by recipients.

By 2024, individuals, care providers, communities and researchers should have an array of interoperable health IT products and services that support continuous learning and improved health. This "learning health system" should also result in lower health care costs (by identifying and reducing waste), improved population health, truly empowered consumers and ongoing technological innovation.

For example, all individuals, their families and health care providers should be able to send, receive, find and use electronic health information in a manner that is appropriate, secure, timely and reliable. Individuals should be able to securely share electronic health information with care providers and make use of the electronic health information to support their own health and wellness through informed, shared decision-making. An interoperable health IT ecosystem should support critical public health functions, such as real-time case reporting, disease surveillance and disaster response, as well as data aggregation for research and value-based payment that rewards higher *quality* care, rather than a higher *quantity* of care.

Section 262 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) defines "health information" as "any information, whether oral or recorded in any form or medium, that (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual." Health information such as personally maintained dietary logs, medical device data such as blood glucose readings and many other bits of information that inform health-related decision-making (both inside and outside the care delivery system) must also be connected in reusable ways in a dynamic ecosystem supported by health IT. Across this ecosystem, electronic health information in its broadest sense is and increasingly needs to be the stuff of everyday decision-making by everyday people.

Scope

For purposes of this Roadmap, interoperability is defined as the ability of a system to exchange electronic health information with and use electronic health information from other systems without special effort on the part of the user.[9] In simple terms, this means all individuals, their families and their health care providers have appropriate access to electronic health information that facilitates informed decision-making, supports coordinated health management, allows individuals and caregivers to be active partners and participants in their health and care and improves the overall health of the nation's population.

The intersection of clinical and administrative electronic health information is a critical consideration, but is out of scope for this version of the Roadmap. Use cases, standards, technologies and tools that leverage both administrative and clinical electronic health information will be an important topic to address in future iterations. There are also many aspects of health IT beyond interoperability that are important and will be critical to a learning health system, including technology adoption,[10] data quality, documentation and data entry, usability and workflow. However, these topics are out of scope for this Roadmap and deserving of separate, dedicated attention. This Roadmap focuses on decisions, actions and actors required to establish the *best minimum level of interoperability* across the health IT ecosystem, starting with clinical health information, in support of a learning health system.

Why a Learning Health System

A learning health system was first conceptualized by the Institute of Medicine (IOM) in 2005 as a Learning Healthcare System, partially in response to its earlier findings in *To Err is Human* and *Crossing the Quality Chasm*. Both of these reports indicated a need for improvements in safety,

A learning health system:

Will improve the health of individuals and populations. This learning health system will accomplish this by generating information and knowledge from data captured and updated over time – as an ongoing and natural by-product of contributions by individuals, care delivery systems, public health programs and clinical research – and sharing and disseminating what is learned in timely and actionable forms that directly enable individuals, clinicians and public health entities to separately and collaboratively make informed health decisions…The proximal goal of a learning health system is to efficiently and equitably serve the learning needs of all participants, as well as the overall public good.

Taken from the *Learning Health Community's Preamble*

---

[9] Derived from the Institute of Electrical and Electronics Engineers (IEEE) definition of interoperability.

[10] Federal Health IT Strategic Plan 2015-2020 Goal One.

efficiency and patient-centeredness of care, based on the best available evidence. IOM envisioned that a Learning Healthcare System would, "generate and apply the best evidence for the collaborative health care choices of each patient and provider; drive the process of discovery as a natural outgrowth of patient care; and ensure innovation, quality, safety and value in health care."[11]

Since 2005, the concept of a learning healthcare system has evolved to the broader concept of a learning *health* system, which extends beyond the care delivery system. A learning health system is an ecosystem where all stakeholders can securely, effectively and efficiently contribute, share and analyze data and create new knowledge that can be consumed by a wide variety of electronic health information systems to support effective decision-making leading to improved health outcomes. A learning health system is characterized by continuous learning cycles at many levels of scale (see Figure 4) and includes a broad array of stakeholders that include the care delivery system, but extend beyond care delivery to public health and the research community. For example, a learning health system includes transactions for routine and emergency public health services among governmental agencies (e.g., state and local health departments, emergency responders and public safety); hospitals; health care professionals; diagnostic laboratories; researchers; and non-governmental social services, advocacy and community based organizations. A learning health system also incorporates advanced health models that increasingly leverage technology, such as telecommunications technology to deliver health and clinical services remotely, that improve access to care across clinical and non-clinical community settings.
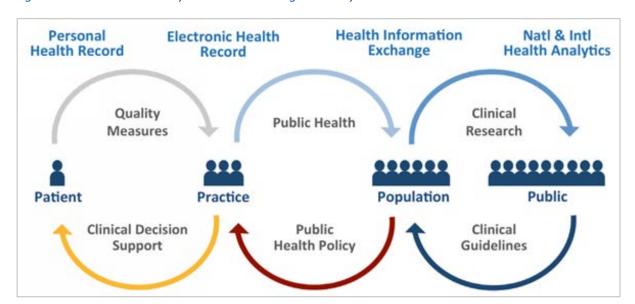
Figure 4: The Health IT Ecosystem as a Learning Health System

---

[11] The Learning Healthcare System: Workshop Summary. Leigh Anne Olsen, Dara Aisner and J. Michael McGinnis. Institute of Medicine. March 2007. http://books.nap.edu/openbook.php?record_id=11903
http://www.learninghealth.org/about-the-community/

Guiding Principles for Nationwide Interoperability

ONC articulated a set of guiding principles and building blocks in *Connecting Health and Care for the Nation: A 10-Year Vision to Achieve an Interoperable Health IT Infrastructure*.[12] Based on feedback from a wide range of stakeholders, ONC has updated these principles as outlined below. These principles should serve as a guidepost in directing not only the critical actions described in this Roadmap, but also as subsequent actions and strategies to advance interoperability in the future. They are intended to focus our collective efforts to make practical and valuable progress, while encouraging innovation.

1. **Build upon the existing health IT infrastructure**. Significant investments have been made in health IT across the care delivery system and in other relevant sectors that need to exchange electronic health information with individuals and care providers. To the extent possible, we will encourage stakeholders to build from existing health IT infrastructure, increasing interoperability and functionality as needed.

2. **One size does not fit all**. Interoperability requires technical and policy conformance among networks, technical systems and their components. It also requires behavior and culture change on the part of users. We will strive for baseline interoperability across health IT infrastructure, while allowing innovators and technologists to vary the usability[13] in order to best meet the user's needs based on the scenario at hand, technology available, workflow design, personal preferences and other factors.

3. **Empower individuals.** Members of the public are rapidly adopting technology, particularly mobile technology, to manage numerous aspects of their lives, including health and wellness. However, many of these innovative apps and online tools do not yet integrate electronic health information from the care delivery system. Electronic health information from the care delivery system should be easily accessible to individuals and empower them to become more active partners and participants in their health and care, just as other kinds of data are empowering them in other aspects of their lives.

4. **Leverage the market**. Demand for interoperability from health IT users is a powerful driver to advance our vision. As delivery system reform increasingly depends on the seamless flow of electronic clinical health information, we will work with and support these efforts. The market should encourage innovation to meet evolving demands for interoperability.

5. **Simplify**. Where possible, simpler solutions should be implemented first, with allowance for more complex methods in the future.

6. **Maintain modularity**. A large, nationwide set of complex systems that need to scale are more resilient to change when they are divided into independent components that can be connected together. Because medicine and technology will change over time, we must preserve systems'

---

[12] http://www.healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf

[13] Usability refers to how useful, usable and satisfying a system is for the intended users to accomplish goals in the work domain by performing certain sequences of tasks. Drs. Jiajie Zhang & Muhammad Walji

abilities to evolve and take advantage of the best of technology and health care delivery. Modularity creates flexibility that allows innovation and adoption of new, more efficient approaches over time without overhauling entire systems.

7. **Consider the current environment and support multiple levels of advancement.** Not every individual or clinical practice will incorporate health IT into their work in the next 3-10 years and not every practice will adopt health IT at the same level of sophistication. We must therefore account for a range of capabilities among information sources and information users, including EHR and non-EHR users, as we advance interoperability. Individuals and caregivers have an ongoing need to send, receive, find and use their own health information both within and outside the care delivery system.

8. **Focus on value.** We will strive to make sure our interoperability efforts yield the greatest value to individuals and care providers; improved health, health care and lower costs should be measurable over time and at a minimum, offset resource investment.

9. **Protect privacy and security in all aspects of interoperability.** It is essential to maintain public trust that health information is safe and secure. To better establish and maintain that trust, we will strive to ensure that appropriate, strong and effective safeguards for electronic health information are in place as interoperability increases across the industry. We will also support greater transparency for individuals regarding the business practices of entities that use their data, particularly those that are not covered by the HIPAA Privacy and Security Rule, while considering the preferences of individuals.

10. **Scalability and Universal Access.** Standards and methods for achieving interoperability must be accessible nationwide and capable of handling significant and growing volumes of electronic health information, even if implemented incrementally, to ensure no one is left on the wrong side of the digital divide.

Who is this Roadmap for?

A learning health system includes the broad range of people and organizations traditionally involved in the delivery of clinical care (providers, individuals, payers) and many outside the care delivery system who impact the health of individuals (e.g., community-based social and human service organizations, schools, the research community, etc.). The following list of stakeholder perspectives is used throughout the Roadmap to denote which stakeholder groups are best positioned to take on a critical action and/or will directly benefit from actions to be taken (Figure 5). In most cases, individuals, groups and organizations fit more than one stakeholder perspective. Furthermore, professional organizations that represent the interests of a particular stakeholder may identify with one or more stakeholder perspective.

Figure 5: Stakeholder Perspectives

People who receive care or support the care of others
Individuals, consumers, patients, caregivers, family members serving in a non-professional role and professional organizations that represent these stakeholders' best interests

People and organizations that deliver care and services
Professional care providers who deliver care across the continuum, not limited to but including hospitals, ambulatory providers, pharmacies, laboratories, behavioral health including mental health and substance abuse services, home and community based services, nursing homes and professional organizations that represent these stakeholders' best interests

Organizations that pay for care
Private payers, employers and public payers that pay for programs like Medicare, Medicaid and Tricare

People and organizations that support the public good
Federal, state, tribal and local governments

People and organizations that generate new knowledge, whether research or quality improvement
Researchers, population health analytics and quality improvement knowledge curators and quality measure stewards

People and organizations that provide health IT capabilities
Technology developers for EHR and other health IT, including but not limited to health information exchange (HIE) technology, laboratory information systems, personal health records, pharmacy systems, mobile technology, medical device manufacturers and other technology that provides health IT capabilities and services

People and organizations that govern, certify and/or have oversight
Governing bodies and accreditation/certification bodies operating at local, regional, or national levels that provide a governance structure, contractual arrangements, rules of engagement, best practices, processes and/or assess compliance

People and organizations that develop and maintain standards
Standards development organizations (SDOs) and their communities of participants, such as technology developers, health systems, providers, government, associations, etc.

How the Roadmap is Organized: Business and Technical Requirements for a Learning Health System

Interoperability Roadmap Building Blocks	LHS Requirements
Rules of engagement and governance	A. Shared governance of policy and standards that enable interoperability: Nationwide interoperability across the diverse health IT ecosystem will require stakeholders to make collective decisions between competing policies, strategies, standards in a manner that does not limit competition. Maintaining interoperability once established will also require ongoing coordination and collaborative decision-making about change
Supportive business, clinical, cultural and regulatory environments	B. A supportive business and regulatory environment that encourages interoperability: Rules that govern how health and care is paid for must create a context in which interoperability is not just philanthropic, but is a good business decision. C. Individuals are empowered to be active managers of their health: A learning health system is person-centered, enabling individuals to become active partners in their health by not only accessing their electronic health information, but also providing and managing electronic health information through mobile health, wearable devices and online services. D. Care providers partner with individuals to deliver high value care: Providers work together with patients to routinely assess and incorporate patient preferences and goals into care plans that achieve measurable value for the individual and the population.
Privacy and security protections for health information	E. Ubiquitous, secure network infrastructure: Enabling an interoperable, learning health system requires a stable, secure, widely available network capability that supports vendor-neutral protocols and a wide variety of core services. F. Verifiable identity and authentication of all participants: Legal requirements and cultural norms dictate that participants be known, so that the context and access to data and services is appropriate. This is a requirement for all individual and organizational participants in a learning health system regardless of role (individual/patient, provider, technician, hospital, health plan, etc.) G. Consistent representation of permission to collect, share, and use identifiable health information: Though legal requirements differ across the states, nationwide interoperability requires a consistent way to represent an individual's permission to share their electronic health information, including with whom and for what purpose(s). H. Consistent representation of authorization to access health information: When coupled with identity verification, this allows consistent decisions to be made by systems about access to electronic health information.

Interoperability Roadmap Building Blocks	LHS Requirements
Certification and testing to support adoption and optimization of health IT products and services	I. Stakeholder assurance that health IT is interoperable: Stakeholders that purchase and use health IT must have a reasonable assurance that what they are purchasing is interoperable with other systems.
Core technical standards and functions	J. Consistent Data Formats and semantics: Common formats (as few as necessary to meet the needs of learning health system participants) are the bedrock of successful interoperability. Systems that send and receive electronic health information generate these common formats themselves or with the assistance of interface engines or intermediaries (e.g., HIOs, clearinghouses, third-party services.) The meaning of electronic health information must be maintained and consistently understood as it travels from participant to participant. Systems that send and receive information may or may not store standard values natively and therefore may rely on translation services provided at various points along the way. K. Standard, secure services: Services should be modular, secure and standards-based wherever possible. L. Consistent, secure transport technique(s): Interoperability requires transport techniques that are vendor-neutral, easy to configure and widely and consistently used. The fewest number of protocols necessary to fulfill the needs of learning health system participants is most desirable. M. Accurate identity matching: Whether aggregated in a repository or linked "just in time," electronic health information from disparate sources must be accurately matched to prevent information fragmentation and erroneous consolidation. As a learning health system evolves, more than individual/patient-specific information from health records will be matched and linked, including provider identities, system identities, device identities and others to support public health and clinical research. N. Reliable resource location: The ability to rapidly locate resources, including individuals, APIs, networks, etc. by their current or historical names and descriptions will be necessary for a learning health system to operate efficiently.

Achieving nationwide interoperability will take a strategic and focused effort by the private sector in collaboration with federal, state, tribal and local governments. Realizing a learning health system that securely, efficiently and effectively gets the appropriate electronic health information to the appropriate person when and where it is needed in a manner that is useful, depends in large part on health IT systems being interoperable.

The Roadmap is based on a core set of business and functional requirements to achieve a learning health system, organized by five critical building blocks that support the business, policies and technical needs of a nationwide interoperable electronic health information infrastructure. These 5 building blocks are interdependent and progress must be incremental across all of them over the next decade:

- Rules of engagement and governance
- Supportive business, clinical, cultural and regulatory environments
- Privacy and security protections for health information
- Certification and testing to support adoption and optimization of health IT products and services
- Core technical standards and functions

A learning health system depends on an ecosystem of nationwide interoperable health IT. Understanding and defining the business and technical requirements of a learning health system helps identify key decisions, actions and actors that must be put into motion, as well as dependencies and relationships that have to be accounted for in the sequencing of activities. Basic functional and business requirements to enable a learning health system are listed below and organized by building block. This is the basic structure of the Roadmap.

Throughout the Roadmap, each requirement has a description of high level historical context, current state, desired future state and critical actions across three-, six- and ten-year timeframes. Each requirement is also linked to the Federal Health IT Strategic Plan objectives it supports, as well as the main stakeholders impacted by the requirement.

Process for Updating the Roadmap

ONC will continue to coordinate efforts and engage with the stakeholders to publish future versions of the Shared Nationwide Interoperability Roadmap. The Roadmap is intended to be a living document that is guided in its evolution by all health and health care stakeholders. ONC has served as the coordinator for this first draft of the Roadmap and will continue to do so for future iterations; however, the owners of the Roadmap are the variety of stakeholders and public represented herein. ONC anticipates updating the Shared Nationwide Interoperability Roadmap every two years with broad input from the public, stakeholders and its federal advisory committees (the HIT Policy Committee and HIT Standards Committee).

For this initial version of the Roadmap, the set of actions described are offered as a starting point. The reader will note there are many objectives that lack one or more critical actions on the road to a learning health system.

As a draft, this Roadmap needs the input from knowledgeable, engaged stakeholders and, in particular, areas where important actions or milestones may be missing, we ask for that input, indicated by the words "stakeholder input requested."

Additional Resources

While the Roadmap contains important detail on each business and functional requirement for a learning health system, there is a significant amount of background that sits behind this document. For more background detail on health IT, as well as learning health system business and functional requirements, please see the resources below.

- Historical background and current progress on interoperability:
    - ONC Report to Congress: Update on the Adoption of Health Information Technology and Related Efforts to Facilitate the Electronic use and Exchange of Health Information, October 2014.
    - ONC Data Briefs
    - ONC Interoperability Portfolio
- Background on ONC's 10 year vision and the five Building Blocks:
    - Connecting Health and Care for the Nation: A 10-Year Vision to Achieve an Interoperable Health IT Infrastructure, August 2014
- Additional information on ONC's Quality Improvement 10 year vision:
    - Health IT Enabled Quality Improvement: A Vision to Achieve Better Health and Health Care, November 2014
- Additional information on APIs and a national architecture for interoperability:
    - JASON Report: A Robust Health Data Infrastructure, April 2014
    - HIT Policy and HIT Standards Committees' JASON Task Force Final Report, October 2014
    - JASON Report: Data for individual health, November 2014
- Additional information on person-centered health care:
    - Person at the Center | HealthIT.gov
- Additional information on patient generated health data:
    - Patient-Generated Health Data | HealthIT.gov
- Additional information on governance:
    - Health Information Exchange | HealthIT.gov
- Appendices within this Roadmap document
    - Appendices

A Shared Nationwide Interoperability Roadmap

This section is organized by building blocks and then LHS requirements that fall under each building block. These building blocks and requirements are described in more detail in the above introduction of this document. Each requirement section contains:

- Information about the requirement and the related Federal Health IT Strategic Plan objectives
- Background information and a summary of the current state
- A 'moving forward' section and critical actions

Rules of Engagement and Governance

A critical component of interoperability is a common set of standards, services, policies and practices that facilitate appropriate electronic health information exchange nationwide. Governance helps identify common policies, operational or business practices, and standards to support services that enable interoperability. Governance can also provide a mechanism for establishing trust across electronic health information trading partners, i.e., confidence in the practices of the other people/organizations with whom electronic health information is shared. While trust can be established among specific, known groups of trading partners through local governance, data use agreements and other contractual arrangements, individuals are mobile and often seek care beyond networks of local trading partners. Thus, it is important to have mechanisms for scaling trust nationwide, which requires assurance that each data holder adheres to a minimum set of common policies, operational and/or business practices and technical standards. Trading partners must also commit to using a common set of technical standards to ensure health IT is appropriately interoperable. A governance mechanism that effectively addresses all of these issues will help advance interoperability across all the diverse entities and networks that comprise a learning health system. This will facilitate the right information getting to the right people at the right time across disparate products and organizations, in a way that can be relied upon and meaningfully used by recipients.

Shared governance of policy and standards that enable interoperability

LHS Requirement:

A. ***Shared governance of policy and standards that enable interoperability:*** Nationwide interoperability across the diverse health IT ecosystem will require stakeholders to make collective decisions between competing policies, strategies, standards in a manner that does not limit competition. Maintaining interoperability once established will also require ongoing coordination and collaborative decision-making about change.

Background and Current State

The need for governance arises anytime a group of people or organizations come together to accomplish an end. In general, "governance is the process by which authority is conferred on rulers, by which they make the rules and by which those rules are enforced and modified."[14] Governance generally includes setting priorities, making decisions, establishing authority(ies) and ensuring accountability.

Governmental Governance to Enable Interoperability

ONC has made several attempts regarding governance to enable the secure nationwide exchange of electronic health information. In 2005, ONC formed the American Health Information Community (AHIC) as a federal advisory committee to discuss how to accelerate the development and adoption of health information technology and the Nationwide Health Information Network (NwHIN).[15] Over the subsequent years, stakeholders and federal agencies worked together to develop the Data Use and Reciprocal Support Agreement (DURSA) for the Nationwide Health Information Network.[16] In 2008, the National eHealth Collaborative (NeHC), a public-private partnership, was established to continue that work and build on the accomplishments of AHIC.

In 2009, the HITECH Act explicitly directed ONC to establish a governance mechanism for the nationwide health information network[17]. In 2012 ONC released a request for information (RFI) on a proposed regulatory approach to governance, titled *Nationwide Health Information Network: Conditions for Trusted Exchange.*[18] The industry response to the RFI indicated a general desire for ONC to refrain from formal governance activity and to allow nascent and emerging governance efforts in industry to take shape. As health information exchange was in its infancy, but growing at a fast pace, commenters were concerned

---

[14] Arriving at a Common Understanding of Governance. The World Bank. http://go.worldbank.org/G2CHLXX0Q0

[15] AHIC worked with organizations like the Markle Foundation to develop principles and frameworks for health information exchange, none of which required adoption or participation by organizations participating in health information exchange.

[16] The DURSA is a single, multi-party agreement that sets the rules by which participants would operate to exchange data.

[17] **SEC. 3001. OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY.** (8) GOVERNANCE FOR NATIONWIDE HEALTH INFORMATION NETWORK.—The National Coordinator shall establish a governance mechanism for the nationwide health information network.

[18] The RFI sought public comment on a regulatory approach to establish a governance mechanism that would create conditions for trusted exchange amongst all of these organizations and set the rules of the road for exchange.

that regulatory action would stifle innovation and improvements in health information exchange. In response to the industry's comments, ONC indicated in September 2012 that it would not move forward at that time with regulation around governance. In 2013, ONC released the *Governance Framework for Trusted Health Information Exchange (HIE)*, which established guiding principles on HIE Governance.[19]

Non-Governmental Governance

In response to increased electronic health information exchange requirements under the EHR Incentive Programs,[20] a number of organizations have been created or enhanced to define policies, practices and standards to enable interoperability between entities in their trust communities and hold participants accountable to these guidelines. Governance organizations that seek to establish exchange across organizational boundaries have also emerged.

Despite significant overlap in the founders and members of these organizations, technical and governance policies that are adopted by each are often incompatible, as are their respective business practices and policies for establishing trust.[21] While the overall objective of each organization is to establish a trust community and enable interoperability, they often have differing immediate goals and differing methods or standards to achieve those goals. While some industries, like airline reservations and ATM networks, only need to support simple use cases and limited standards, the health care industry is much more complex (see Appendix H for Priority Interoperability Use Cases). Some networks that support health care depend upon legal data sharing and use agreements, while some rely on self-attestation or independent accreditation. Some operate testing programs while others do not. And most (but not all) operate some level of technical infrastructure to identify participants in the trust community.

In addition to varying policies and business practices that establish additional constraints beyond applicable law and regulation, there is also significant variation in the technical standards these organizations use to support interoperability, including specifications for content, transport and security. Organizations often have overlapping regional, state or national footprints, sometimes establishing trust communities that may compete for members. Additionally, some vendors and organizations have chosen not to participate in any of these organizations due to uncertainty about the industry and ONC's direction, or due to the costs associated with participation. The result is a complex web of electronic health information sharing arrangements that create some degree of interoperability within specific geographic, organizational and vendor boundaries, but fail to produce seamless nationwide interoperability to support a learning health system.[22]

---

[19] http://www.healthit.gov/sites/default/files/GovernanceFrameworkTrustedEHIE_Final.pdf

[20] Criteria include a requirement that eligible hospitals, critical access hospitals and eligible professionals send electronic care summaries for transitions of care and enable their patients to transmit care summaries electronically.

[21] Interoperability Workgroup Governance Subgroup Presentation. July 2014. http://healthitgov.ahrqstg.org/facas/sites/faca/files/GSG_Slides_2014-07-23%20final_0.pptx

[22] Ibid.

Standards Development

In addition to the governance actors, there are standards development organizations (SDOs) that develop technical standards and implementation guidance for content, semantics and transport of health information.[23] While these entities serve a governance role for standards, there are important differences between them and broader governance functions related to technical standards. Unlike governance organizations, which tend to address the same subject matter and focus on constraint and guidelines to enable interoperability, SDOs work toward the establishment of particular types of standards.

In addition to the standards work done by SDOs, there are entities that work to establish guidelines and constraints in the use of standards developed by SDOs.[24] The S&I Framework[25] in particular has worked to prioritize new standards initiatives and identity needs for constraining implementation guides. In most cases, the newly developed or constrained standards have then been picked up by SDOs and managed per their normal processes.

Moving Forward and Milestones

While the various organizations with their varying governance methods (policy, operational and technical) described above play an important part in the governance landscape, there is no single process or mechanism to bring them all together in a coordinated manner or in a manner that can reconcile differences. Furthermore, additional networks will likely emerge as customer needs evolve. The challenge is finding a way for health information to flow between these networks with varying policies and architectures.

It is important that there be a set of "rules of the road," a multi-stakeholder process to address operational issues to support the rules of the road and a mechanism for demonstrating and identifying compliance with the rules, as well as addressing non-compliance. A coordinated governance mechanism must support a transparent and inclusive process for identifying operational issues and making decisions to support electronic health information exchange for individual and population health. The process should be inclusive of public and private actors and must hold true to the principle of person-centeredness.

---

[23] SDOs do not necessarily work on the standards that the industry, CMS, ONC and other federal agencies believe are necessary to support interoperability. SDOs are member-based organizations and those members set the priorities for which standards will be developed and refined. Each SDO has a very refined process for developing, balloting, piloting, finalizing and maintaining standards and that piece of the process is working well. However, requirements development, priority setting (meaning what standards to focus on), implementation oversight, accepting feedback and enforcing correct implementations of the standards are not necessarily aligned with the priorities of health information exchange organizations.

[24] One such organization is the EHR│HIE Interoperability Work Group (IWG). Some efforts of the IWG have been considered by the responsible SDO and resulted in important updates.

[25] http://wiki.siframework.org/

To implement this process, there needs to be a set of criteria for entities that facilitate electronic health information interoperability (exchange and use) to follow. The federal government has a role to play in establishing rules of the road that support consumer protection and availability of electronic health information for individual and population health and supporting these rules and any specific governance criteria or accountability mechanism through its programs and requirements.

The private sector has a key role to play in coalescing behind a common coordinated governance process that will establish or refine the criteria that support interoperable health IT. The public and private sectors must work together to identify and address operational issues that currently inhibit interoperability. The public and private sectors also must establish a mechanism for compliance and accountability to governance criteria. In instances where the process has established consensus criteria that require additional reinforcement, ONC or other federal agencies will consider creating implementation specifications for the criteria that could be adopted through existing public programs.

Governance Principles

Governance should address three main subject matter areas: policy, operations and technical standards. There needs to be a single set of basic rules of the road to support interoperability nationwide and address consumer protection. The set of principles below represents a foundation that should endure over time. More detailed criteria that support these principles can be established to support different interoperability needs as they emerge over the next three, six and ten years. These principles are based on the Governance Framework for Trusted Electronic Health Information Exchange, fair information practice principles, established privacy and security policy, and build on the existing legal framework for health information.

Policy

Figure 6: Overview of Governance Principles

- **Access to Personal Health Information**: Data holders and entities facilitating interoperability of health information shall, in accordance with applicable law and individual preferences, exchange information, including with the individual to support patient care, care coordination and other permitted purposes. Specifically:
  - No policy, business, operational, or technical barriers that are not required by law should be built to prevent information from appropriately flowing across geographic, health IT developer and organizational boundaries in support of patient care.
  - Where individuals clearly instruct a data holder to release information about them to others, the data holder should comply with that directive.
  - Data holders and entities that facilitate interoperability should not compete on the

GOVERNANCE PRINCIPLES:
"Rules of the Road"

POLICY

OPERATIONS

STANDARDS

availability of patient health data.

- o Promote collaboration and avoid instances where (even when permitted by law) differences in fees, policies, services, operations or contracts would prevent individuals' personal health information from being electronically exchanged.

- **Respect Policies of Other Exchange Partners:** Data holders and entities facilitating interoperability of electronic health information should not establish policies or practices in excess of law that limit the availability of electronic health information by another entity that is in compliance with applicable laws and these governance principles.

- **Individual Choice:** Data holders and entities facilitating interoperability of health information should grant individuals, consistent with existing law, the ability to exercise choice over what personal health information these organizations collect from them and how the organizations use it and share it.

  - o An individual shall not be denied access to health care services based on whether they have documented their choice regarding electronic health information exchange.
  - o Individuals retain the right to not disclose their information in the first instance.
  - o Data holders and entities that facilitate the interoperability of health IT should provide clear and simple choices regarding what restrictions an individual can and cannot place on the collection, sharing, or use of that individual's health information. These choices should be presented at times and in ways that enable individuals to make meaningful decisions about personal health information collection, use and disclosure. These choices should be presented at an appropriate level for the literacy and language preference of the individual.
  - o Data holders and entities that facilitate the interoperability of electronic health IT should enable these choices by providing individuals with easily used and accessible electronic processes that reflect the scale, scope and legal sensitivity of the personal health information that data holders collect, use, or disclose as well as the legal sensitivity of the uses they make of the information.

- **Transparency:** Data holders and entities facilitating electronic exchange of health information should provide easily understandable and accessible information about organizations' data practices. Specific examples include, but are not limited to:

  - o Data holders and entities should provide clear descriptions of what personal health information they collect, why they need the data, how they will use it, when they will delete it or de-identify it and whether and for what purposes they may share such data.
  - o Data holders and entities should provide clear descriptions of decision tools that may be used to match individual identifying information, share individually identifiable information, or withhold individual identifying information sharing.
  - o Data holders and entities should provide clear information to health information trading partners about technical error rates (e.g., for improper individual matching) and other information (for example results of independent audits of security controls) about information interoperability that may have diverged from expected practices.

- **Security**: Data holders and entities facilitating interoperability of health information should secure and ensure responsible handling of personal health information in line with other examples of critical infrastructure. Specific examples include but are not limited to:
  - Data holders and entities should maintain reasonable safeguards to control risk, such as loss, unauthorized access, use, destruction, or modification and improper disclosure.
  - Data holders and entities should ensure that an individuals' personal health information is consistently and accurately matched when electronically exchanged.
  - Data holders and entities should take reasonable steps to ensure that personal health information is complete, accurate and up-to-date to the extent necessary for the intended purpose and has not been altered or destroyed in an unauthorized manner.
- **Individual Access and Correction**: Data holders and entities facilitating exchange of health information should provide individuals, consistent with applicable laws, a means to exchange and obtain electronic access to personal health information and the ability to correct such information in a timely manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to the individual if the data is inaccurate.

Operations
- **Transparency**: Entities facilitating interoperability of health IT should operate with transparency and openness, including making publicly available information describing their electronic exchange capacity and services, for example: number of users, the types of standards implemented, number of patient lives covered and transaction volume.
- **Inclusive Governance**: Entities facilitating interoperability of health IT should promote inclusive participation and adequate stakeholder representation (especially among individuals and patient advocates) in the development of data policies and operations policies.
- **Open Exchange**: There should be neutrality in the exchange of personal health information.
  - An entity engaged in the exchange of electronic health information shall treat all personal health information exchange requests, services and efforts in roughly the same way and not erect barriers to the authorized flow of information. For instance, a health IT developer that has health information exchange applications shall not prevent a user from using health information exchange applications developed by competitors.
  - Provide open access to exchange services, such as access to an organization's provider directory that would enable local, regional and/or nationwide organizations and individuals to identify with whom they can electronically exchange information and how such exchange would have to be completed, pursuant to applicable laws and regulations.

Standards
- Data holders and entities facilitating exchange of electronic health information should ensure standards are prioritized, developed and implemented to support the public interest, national priorities and the rights of individuals (e.g., health care delivery, privacy).
  - Where available and appropriate for the desired exchange of health information federal vocabulary, content, transport and security standards and associated implementation specifications are used.

- o Standards should support data portability from one health IT product to another.
- o The development and implementation of technical requirements should enable the adaptation and incremental evolution of health information exchange and technologies supporting exchange to meet current and future needs of users as standards evolve.
- o Standards development and adoption should not unfairly provide an advantage to one sector or one organization over others.

Table 1: Critical Actions for a Coordinated Governance Framework and Process for Nationwide Health Information Interoperability

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
A1. Establishment of Coordinated Governance	1. ONC will define a nationwide governance framework with common rules of the road for trust and interoperability and a mechanism for identifying compliance with common criteria. These rules will first focus on interoperability of a common clinical data set for purposes of treatment. 2. ONC will identify a mechanism for recognizing organizations that comply with the common rules of the road. 3. **Call to action: Public and private sector stakeholders across the ecosystem should come together to establish a single coordinated governance process to establish more detailed policies regarding business practices, including policies for identifying and addressing bad actors and to identify the technical standards that will enable interoperability for specific use cases** (see Appendix H for Priority Interoperability Use Cases). 4. **Call to action: Federal agencies that provide or pay for health services should align their policies for interoperability with the nationwide governance framework.** 5. ONC and stakeholders participating in the coordinated governance process should establish metrics for monitoring and assessing nationwide interoperability and methods for data collection.	6. The coordinated governance process will continue to operate and update policies for business practices/operations and technical standards to enable interoperability as needed. 7. ONC and stakeholders will use nationwide interoperability metrics to assess the success of governance activities and make or recommend changes, as needed.	8. The coordinated governance process will continue to operate and update policies for business practices/operations and technical standards to enable interoperability as needed. 9. ONC and stakeholders should continue to use nationwide interoperability metrics to assess the success of governance activities and make or recommend changes, as needed.

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
A2. Policies & Operations	1. Governance entities and data holders should align their policies with the nationwide governance framework. 2. ONC, in collaboration with stakeholders, should define a policy framework for exchange of patient-generated health data and pilot it.	3. ONC will work with the established coordinated governance process to identify or modify criteria and implementation specifications to address an expanded data set and uses of health information beyond treatment, including but not limited to payment and health care operations and patient-generated health data. 4. ONC and stakeholders participating in the coordinated governance process, human service providers and health-related device overseers should define policies for interoperability of health information from non-clinical sources. 5. ONC and stakeholders participating in the coordinated governance process should define a policy framework for interoperability of clinical data to support research and big data analyses.	6. ONC will work with the coordinated governance process to identify or modify criteria and implementation specifications to address the needs of a learning health system. 7. ONC and stakeholders participating in a coordinated governance process should define criteria and implementation specifications for interoperability of clinical data to support research and big data analyses nationwide.

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
A3. Standards	1. The coordinated governance process should support three main functions related to technical standards: prioritization of use cases for which standards are needed, selection of standards to support priority use cases based on ONC's Interoperability Advisories and coordination across SDOs and implementers as standards are developed and refined (see Appendix H for Priority Interoperability Use Cases). 2. The coordinated governance process should support a holistic lifecycle process for technical standards that enable care providers and individuals to send, receive, find and use a common clinical data set. This involves establishing clear feedback loops between SDOs and implementers, as well as supporting non-certification-related testing of technical standards.	3. The coordinated governance process should establish an ongoing evaluation process for the efficacy of standards and testing tools. 4. The coordinated governance process should work with SDOs to identify or develop additional standards for new learning health system priority functions as part of the holistic lifecycle process. 5. The coordinated governance process should use the standards evaluation process on an ongoing basis to coordinate the roll out of software and service changes so as not to disrupt established interoperability.	6. The coordinated governance process should continue to evaluate the efficacy of standards and testing tools. 7. The coordinated governance process should continue to use the standards evaluation process on an ongoing basis to coordinate the roll out of software and service changes so as not to disrupt established interoperability.

Supportive Business, Clinical, Cultural and Regulatory Environments

While the Medicare and Medicaid EHR Incentive Programs have been a primary motivator for the adoption and use of certified EHR technology, these programs alone are insufficient to overcome barriers to our vision of information sharing and interoperability as outlined above. Current policies and financial incentives often prevent such exchange, even when it is technically feasible. To ensure that individuals and care providers send, receive, find and use a basic set of essential health information across the care continuum over the next three years, we need to migrate policy and funding levers to create the business imperative and clinical demand for interoperability and electronic health information exchange.

A Supportive Business and Regulatory Environment that Encourages Interoperability

LHS Requirement

B. ***A supportive business and regulatory environment that encourages interoperability:*** Rules that govern how health and care are paid for must create a context in which interoperability is not just a way to improve care, but is a good business decision.

FEDERAL HEALTH IT STRATEGIC PLAN OBJECTIVES SUPPORTED

▸ Improve health care quality, access and experience through safe, timely, effective, efficient, equitable and person-centered care
▸ Support the delivery of high-value health care
▸ Improve clinical and community services and population health
▸ Increase access to and usability of high-quality electronic health information and services

---

Policy and funding levers that create the business imperative for interoperability are pivotal for helping to ensure that individuals, caregivers and providers can send, receive, find and use a common clinical data set across the care continuum in the near term. Policy levers related to other learning health system stakeholders such as public health, social and human services and research communities must also be addressed. Additionally, a cultural shift at both the individual and provider levels is necessary to empower individuals to participate in their health and care.

Background and Current State

Despite strong agreement on the need for interoperability to enable higher quality, more efficient, person-centered care, the demand among providers, consumers and purchasers of health care has not yet translated into seamless interoperability across the health care system. Countervailing market forces and structural attributes of the health care system make it costly to move away from the status quo of fragmented care and silos of health information, inhibiting widespread adoption of interoperable systems. One key barrier to interoperability arises from the way in which health care in the U.S. has

traditionally been reimbursed (typically "fee-for-service" payment models.) Economic gains from interoperability are realized in the form of greater efficiency in the delivery of health care—for instance, laboratory and imaging tests are often duplicated when an existing image that might obviate the need for a test is not available or not accessed, contributing to wasteful health care spending that could be allocated more efficiently. While the effective use of interoperable systems has the potential to address this waste by allowing providers to share test results, there are few incentives to adopt these systems under the fee-for-service system, which can actually incentivize providers to deliver a greater volume of services and disincentivize the reuse of prior lab tests.

In addition, many market participants, especially those in health care markets characterized by intense competition, may be wary of how increased interoperability will impact their business strategy and competitive position. Providers are concerned about increased liability risk when they exchange health information outside their walls and they may not view the benefits associated with interoperability as outweighing the costs of ensuring that they are exchanging information in a secure fashion that adequately protects individuals' information. Seamless interoperability could also enable individuals and their caregivers to more easily change care providers and transfer electronic health information among providers, thereby reducing providers' competitive advantages from exclusive access to an individual's health information.

These same forces may impact health IT vendors' behavior, reinforcing a status quo characterized by high costs to switch products and services, greater lock-in and reduced data portability. The lack of economic incentives for coordinated and efficient care across the continuum has fostered a health IT market where providers have demanded tools that meet their organization's internal care delivery needs but not tools that are person-centered in allowing interoperability across many different settings and providers of care. Moreover, providers interested in improving interoperability are in some cases limited by their vendor agreements in demanding interoperability. Experience from the REC program[26] has shown small providers making purchasing or licensing decisions often lack the time and resources to keep up with emerging health IT trends and products. Furthermore, interoperability and data liquidity could enable providers to more easily change health IT vendors, increasing competition between vendors.

Finally, the fragmented nature of the health care marketplace poses fundamental challenges to interoperability. Where other industries have captured efficiencies from common standards and shared infrastructure, they have often relied on the market power of a few major actors that are able to drive standardization by virtue of their size and reach. Certain care delivery organizations may be dominant in a local or regional market, but have little presence elsewhere, while large payer organizations may have national reach but only a limited presence in any given market. Within this landscape, the federal government is unique in its market reach, but is still limited in its capacity to drive standardization.

---

[26] The Regional Extension Center (REC) program provides implementation assistance to priority practices—those with limited financial, technical and organizational resources—but the assistance is time limited. Link to study: http://www.annfammed.org/content/13/1/17.full

Achieving greater interoperability, with common policies and standards, will require coordinated commitments across health care stakeholders to overcome these fragmentation challenges.

Over the past several years, the public and private sector alike have made progress toward changing the way health care is paid for, laying the groundwork for a value-based and person-centered health system. Under new "value-based payment" programs, providers are reimbursed based on the quality of care delivered and the degree to which providers can keep costs low and increase efficiency. These programs strengthen the business imperative to adopt common standards and exchange information across the care continuum to provide more coordinated and effective care.

With value-based payment, having up-to-date information to support individuals is critical for providing timely and necessary care and services. For example, knowing that a discharged patient with congestive heart failure is gaining weight the week after they are discharged can trigger home-based interventions that can help prevent the patient from being readmitted, saving significant costs overall and preventing negative patient outcomes. Models that emphasize shared accountability for value across different organizations, including non-traditional stakeholders such as community-based services, are also creating incentives to seamlessly share information with partners.

However, paying for outcomes alone will not be sufficient to change the way providers deliver care. The transition to value-based payment is a long-term, incremental process and providers will need to master new tools and ways of working together before they are willing to take on more substantial levels of risk. Payment policy should encourage incremental steps toward interoperability and address those disincentives that stakeholders perceive as making the transition to interoperability too costly.

While the Medicare and Medicaid EHR Incentive Programs (EHR Incentive Programs) have provided significant incentives to adopt health information technology that can share information according to common standards, further action may be needed to counter the powerful business drivers described above. In addition, the EHR Incentive Programs were not designed to include all providers across the continuum of care, such as long-term care and behavioral health providers, which are some of the most significant cost drivers in the care delivery system.

As HHS continues to test and advance new models of care that reward providers for outcomes, it will help to create an environment where interoperability makes business sense. Additional policy levers across the public and private sector could also be leveraged to encourage interoperable health IT, including: 1) new incentives to adopt and use interoperable health information systems to create additional demand for interoperability; and 2) requirements/penalties that raise the costs of not moving to interoperable systems.

Moving Forward and Critical Actions

To achieve this vision, all stakeholders who pay for health care must explore opportunities to accelerate interoperability as a key component of broader efforts to move toward a value-based healthcare system. The following discussion focuses on ways the federal government, state governments, commercial payers

and health care purchasers can contribute to creating an interoperable, learning health system over three-, six- and ten-year periods, by creating a supportive business and regulatory environment.

Federal Government (See Appendix A for additional information)
As the nation's largest payer, as well as a significant purchaser of health care, the federal government can exercise considerable leverage across the care delivery system to increase demand for interoperability. HHS, as the agency responsible for the Medicare and Medicaid programs, plays a crucial role in advancing the regulatory environment for interoperability.

In the August 2013 document *Principles and Strategy for Accelerating HIE*, HHS articulated a commitment to leveraging appropriate authorities that go beyond HITECH implementation to accelerate interoperability and the electronic exchange of health information across the health care system.[27] As discussed in the document, HHS will pursue a natural lifecycle of policies to drive interoperability beginning with incentives, followed by payment adjustments and then conditions of participation in Medicare and Medicaid programs. HHS is now pursuing ways to promote interoperability as a core element of delivery system reform for providers across the country. An important recent policy demonstrating this commitment is the separately billable payment for chronic care management, finalized under the 2015 Physician Fee Schedule. In order to bill for these services, physicians will be required to utilize certified health IT to furnish certain services to beneficiaries.[28]

Today, federal value-based payment programs have already begun to advance the business case for improved care coordination through interoperable health IT. Accountable care programs, which encourage doctors and hospitals to reduce the growth of total cost of care for individuals in exchange for an opportunity to share in savings, are designed to reward more effective care coordination. In the next three years, HHS can look to reinforce interoperability among providers participating in these programs through measures of adoption of health IT among providers. As market capabilities around interoperability mature, programs may transition to measures more directly focused on interoperability.

Other federal partners that purchase health care, such as the Department of Defense and the Office of Personnel Management, can also advance interoperability by promoting use of measures of health IT adoption and interoperability in a consistent fashion across contracted payer organizations' provider networks. In addition to health plans, federal contracts and grants often support acquisition of health IT infrastructure and services across a wide range of agencies. HHS can work with selected agencies to ensure funding streams for capital investments for health information systems include consistent requirements around interoperability standards.

---

[27] http://www.healthit.gov/sites/default/files/acceleratinghieprinciples_strategy.pdf

[28] CY 2015 Revisions to Payment Policies under the Physician Fee Schedule and Other Revisions to Medicare Part B. CMS-1612-FC. November 2014. http://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/PhysicianFeeSched/PFS-Federal-Regulation-Notices-Items/CMS-1612-FC.html

State governments are key partners in advancing a business environment that is supportive of interoperability and reinforces information exchange. Through the administration of state Medicaid programs and their ability to direct how federal Medicaid funds are spent, states have considerable opportunities to support interoperability. The Centers for Medicare and Medicaid Services (CMS) has identified a number of ways that states can use Medicaid funds to develop care coordination capacity among their Medicaid providers. Several states have already begun to use Medicaid Managed Care contracts to advance interoperability. As part of managed care organization requests for proposals (RFPs) and contracts, states can require payers to ensure that provider networks use interoperable health IT or electronically report data to support care coordination as a condition of participation. States can also emphasize use of health IT and health information exchange as part of quality strategies for managed care plans.

States have a number of opportunities to direct Medicaid funding to subsidize interoperable infrastructure. Integration of health information exchange and health IT into state Medicaid programs can be accomplished under demonstration authority at section 1115 of the Social Security Act[29] (1115 demonstrations). States can also use the State Plan Amendment process to integrate health IT and health information exchange within their Medicaid state plans. Several states implementing health homes have done this to ensure health information exchange is enabling care planning and/or care coordination and successful implementation of their programs. Finally, through the Medicaid funding available under the HITECH act, states can receive funding for administrative activities related to core health information exchange services (e.g., designing and developing a provider directory, privacy and security applications and/or data warehouses), public health infrastructure, electronic clinical quality measurement (eCQM) infrastructure and provider on-boarding.

In addition to leveraging federal funding, states can use independent authorities in a variety of ways to drive interoperability. Many states have already established state-level policy and programs to promote interoperability, for instance, by mandating connection to health information exchange services, setting interoperability requirements at the state level, or setting aside dedicated funding streams for exchange infrastructure. Other states are operating health information exchange services directly, according to standards-based approaches (as either a health information exchange or health care provider), or using their convening powers to encourage interoperability across state-level stakeholders.

The critical actions in the Table 2 below illustrate how states could use these levers to advance interoperability across the country over time.[30]

---

[29] http://www.ssa.gov/OP_Home/ssact/title11/1115.htm

[30] States have clearly communicated that they wish to have an ongoing relationship with ONC to work on the implementation of the Nationwide Interoperability Roadmap. See ONC's State Engagement on the Interoperability & Exchange Roadmap - Summary Report and Findings.

Much like public payers, commercial health plans have an important role to play in driving accountable care and value-based payment. Interoperability among provider networks can offer important competitive advantages to payers seeking to ensure members have access to high-value, coordinated care. These attributes of provider networks are also attractive to health care purchasers seeking to partner with networks that can deliver the most efficient care for employees.
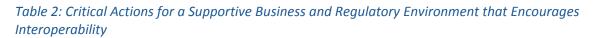
In parallel with public sector efforts over the past several years, commercial payers have developed and deployed a wide range of value-based payment programs within their provider networks that offer new opportunities to focus attention on and generate demand for interoperability. For instance, payers can make adoption of certified health IT systems or demonstration of interoperability a condition of participation for providers that wish to take part in these programs. In markets with more advanced infrastructure for health information exchange, such as an active health information organization, payers could consider partnering with a health information organization and requiring participation by providers seeking to join these programs.

Outside of value-based payment, payers could also focus on incentivizing consumers to choose providers within their networks that have advanced IT-enabled capabilities around care coordination, similar to current measures that seek to drive consumers toward providers that deliver high-value services. Commercial payers could also explore adding health IT and interoperability requirements to the factors included as part of credentialing processes for providers in their networks. Finally, alignment across payers around value-based payment programs and reporting requirements can help providers understand individuals' total cost of care and reduce administrative burden related to managing multiple value-based programs.

Purchasers

Private purchasers of health care, including large employers, can also contribute to a supportive environment for interoperability. Purchasers can selectively contract with plans that demonstrate a commitment to the use of interoperable health IT and health information exchange among network and non-network providers (e.g., certain percentage meeting meaningful use requirements or engaging in health information exchange). Purchasers can also commit to sponsoring benefit plans that encourage employees to choose providers that are using interoperable health IT and support individual access to electronic health information.

Finally, purchasers, especially those with a large economic presence in a given market, can act as a powerful force to support state and community- based efforts to advance use of interoperable health IT by collaborating with other purchasers, providers and consumers.

Table 2: Critical Actions for a Supportive Business and Regulatory Environment that Encourages Interoperability

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
B1. Federal Actions	1. CMS will aim to administer 30% of all Medicare payments to providers through alternative payment models that reward quality and value, rather than volume, by the end of 2016. Alternative payment models may increasingly require a baseline level of health IT adoption or other provisions reinforcing interoperability. 2. Federal agencies will begin to incorporate technical standards and certification requirements in new grants and contracts that fund health IT adoption and Medicaid financing of IT systems. 3. CMS will encourage states to emphasize provider networks' health IT adoption and interoperability to support care coordination as a component of state oversight of Medicaid Managed Care required quality strategies, performance measurement reporting, etc. 4. ONC will reinforce the ability of individuals and providers across the care continuum to send, receive, find and use a common clinical data set through its funding programs.	5. CMS will aim to administer 90% of fee-for-service Medicare payments with a tie to quality or value, including aligned e-clinical quality measures reported from certified health IT by the end of 2018. 6. CMS will aim to administer 50% of all Medicare payments to providers through alternative payment models that reward quality and value by the end of 2018. Value based payment will foster standards based-exchange to support care coordination and quality improvement. 7. The federal government reinforces safe transitions of care facilitated by the timely electronic exchange of necessary, standardized clinical data by considering new Conditions of Participation and/or guidance through surveys and certification. 8. A significant portion of active federal grants and contracts that include provisions related to health IT adoption and exchange align with national standards for health IT.	9. Federal government will use value-based payment models as the dominant mode of payment for providers and require use of interoperable health IT tools. 10. Through conditions of participation in Medicare, the federal government recognizes use of interoperable health IT and standards-based exchange consistent with clinical and safety statutory requirements. 11. Purchasers, including the federal government, include consistent requirements around health IT adoption and health information exchange use among contracted plans' network providers in a manner that does not limit competition.

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
B2. State Actions	1. Call to action: All states should have an interoperability roadmap articulated in their health-related strategic plans (including their Annual Medicaid Health IT Plan). 2. Call to action: All states should take appropriate steps to implement policies that are in alignment to the national, multi-stakeholder approach to coordinated governance for interoperability. 3. Call to action: Roughly half of states should have proposed and/or implemented strategies to leverage Medicaid financial support for interoperability. 4. Call to action: Roughly half of states should enact state-autonomous policies to advance interoperability that go beyond their current efforts. 5. Call to action: All states should utilize health homes or other new models of care and payment to integrate behavioral health with physical health and incentivize health information exchange.	6. Call to action: States with managed care contracts should routinely require provider networks to report performance on measures of standards-based exchange in required quality strategies, performance measurement reporting, etc. 7. Call to action: States should implement models for multi-payer payment and health care delivery system reform. 8. Call to action: A majority of states should act upon Medicaid financial support opportunities for interoperability and exchange. 9. Call to action: The vast majority of states should enact state-autonomous policies to support interoperability.	10. Call to action: All states should use initiatives around value-based arrangements under Medicaid to provide electronic tools to improve care coordination and deliver quality improvement data to providers.
B3. Private Payer/ Purchaser Actions	1. Call to action: A growing number of private payers should implement provisions supporting interoperability within value-based payment arrangements covering commercial populations. 2. Call to action: Purchasers should consider health plans' commitment to the use of interoperable health IT and health information exchange among network and non-network providers in their purchasing decisions.	3. Call to action: Private and public payers should align on common performance measures for interoperability and exchange for incorporation into value-based models.	4. Call to action: Public and private payers should be unified around a common approach to administering value-based models. 5. Call to action: Access to seamless and secure patient data across the continuum of care should be a fundamental component of payments delivered through value-based mechanisms.

Individuals Are Empowered, Active Partners in Their Health and Health Care

LHS Requirement

C. *Individuals are empowered to be active managers of their health*: A learning health system is person-centered, enabling individuals to become active partners in their health by not only accessing their health information, but also providing and managing health information through mobile health, wearable devices and online services.

FEDERAL HEALTH IT STRATEGIC PLAN OBJECTIVES SUPPORTED

▸ Improve health care quality, access and experience through safe, timely, effective, efficient, equitable and person-centered care
▸ Improve clinical and community services and population health
▸ Empower individual, family and caregiver health management and engagement

---

Background and Current State

Today, in many health care settings, an individual is often more of a recipient of health care services than an active partner with their care providers and care team. This dynamic limits the opportunities for people to actively manage their own health and to participate in shared decision making about their care. The ability of individuals to access and use their health information electronically and to contribute health information about themselves serves as one of the cornerstones of nationwide efforts to increase individual engagement and improve health outcomes. Historically and even today, individuals have not had easy access to their health records. To obtain copies, individuals often have to face the inconvenience of going to a medical records department in person, signing forms and paying a fee to obtain their records. Achieving progress in this area relies on concurrent changes across health care providers, individuals, national policies, state and federal laws and health IT.

Over the last few years, policy changes have been put in place to increase consumer's access to their electronic health records and, increasingly, many are taking advantage of this access. In fact, in 2013, among those given access to their online record, almost half viewed their online health information at least once within the previous year. Three quarters of those individuals who did access their health information online used it to monitor their health and four in10shared their electronic health information with someone else.[31] However, challenges persist for some individuals, such as those in underserved communities, partly due to disparities in technology access and digital literacy. Further, individuals' behavioral health data, social and community service data and the data of those who reside in long-term, post-acute care settings are still often unavailable electronically.

---

[31] Individuals' Access and Use of their Online Medical Record Nationwide: ONC Data Brief #20. September 2014. http://www.healthit.gov/sites/default/files/consumeraccessdatabrief_9_10_14.pdf

Though individuals are receiving increased access to their records, significant progress still needs to be made to enable individuals to be true partners in their health and care, supported by information and technology. Patient health information is often spread across multiple providers using disparate IT systems making it cumbersome for consumers to collect, share and use their health information. A number of initiatives have been implemented over the last few years to help individuals access and use their health information, particularly their electronic health information, including:

- Meaningful Use stage 2 patient and family engagement measures;
- ONC's Blue Button campaign;
- the Investing in Innovation (i2) program; and
- coordinated work on policies and technology to support patient-generated health data and personalized care.

Additionally, care planning, which includes individual goals and preferences, is increasingly used and recognized as an integral tool for coordinating patient care, particularly for persons with chronic conditions and multiple co-morbidities. These efforts are described in more detail in Appendix B.

Moving Forward

While the concept of "patient-centered health care" has been emerging over the past decade, there is vast distance between that concept and a truly "person-centric" vision that embraces the value of the individual inside and outside the health care system for improving both health and care. There needs to be a greater focus on incorporating patient-generated health data and ensuring the availability of tools for individuals to use this information to manage their health and make more informed health-related decisions. In the future, there will be increased numbers of at home and community-based services and information from these sources will need to be incorporated or connected with institutionally based clinical information. Changing the paradigm to a person-centered ecosystem is vital to improving health given that an individual's actions greatly impact health outcomes. The person-centered care vision is that, "the power of each individual is developed and unleashed to be active in managing their health and partnering in their health care, enabled by information and technology."[32]   Providers, government, payers and health IT developers have a role in supporting and empowering individuals to become effective managers of their health and wellness where they live, work and play, using information and technology.

---

[32] http://www.healthit.gov/policy-researchers-implementers/person-center

Table 3: Critical Actions for Individuals That Are Empowered, Active Partners in the Health and Health Care

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
C1. Cultural change for individuals including demanding and using their electronic health information	1. Call to action: A majority of individuals and their caregivers should demand access to their electronic health information in a format they can use to manage their health or that of others.	2. Call to action: An increasing proportion of individuals and caregivers should demand and ask for access to their electronic health information in a format they can use to manage their health or that of others. 3. Call to action: Individuals should contribute clinically relevant patient-generated health data and request corrections to their electronic health information to effectively manage their interactions with the care delivery system and to manage their health and wellness where they live, work and play. 4. Call to action: Individuals and their extended care teams (including family and caregivers) should utilize care planning to capture individual goals and preferences as part of longitudinal health information used across care settings.	5. Call to action: Individuals should regularly access and contribute to their health information in health IT, send and receive electronic health information through a variety of emerging technologies and use the information to manage and participate in shared decision making with their care team.

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
C2. Providers and technology developers supporting individual empowerment	1. ONC, government and the industry will identify best practices for the incorporation of patient-generated health data in health care delivery. 2. Call to action: Providers should encourage their patients to access their health information online and will enable patients to view, download and transmit that information to a destination of the patient's choice. 3. Call to action: Providers and technology developers should provide a majority of individuals with the ability to send and receive their health information and make decisions with the providers of their choice, including but not limited to their existing care team based on their preferences 4. ONC will work with the technology community to increase the use of Blue Button through implementation of a portfolio of standards to support consistency in the way that individuals receive information. 5. ONC and government ensure that patients understand their ability to access, send and receive health information.	6. Call to action: Providers and technology developers should support the incorporation of patient-generated health data in health care delivery, which may include advance directives, remote monitoring, glucose levels and other data individuals are tracking 7. Call to action: Technology developers should deploy innovative aggregation platforms and tools that allow individuals and caregivers to receive and compile health information from multiple sources in one place, send their data to a destination of their choice and find and use the information they need (as determined by the individual), to support for example, the individual participating in shared decision-making with their care team. 8. Call to action: Providers should welcome and use information from other providers to avoid duplication of tests and ensure coordinated care.	9. Call to action: Providers and health IT developers should provide a majority of individuals/caregivers the ability to contribute as needed to their electronic health information and support the incorporation of patient-generated health data.
C3. Privacy and Security for Individuals	1. Call to action: Public and private sector stakeholders should assess whether people understand how to safeguard their health information and the need for resources related to this topic. 2. Call to action: Providers should provide individuals with secure access to their own behavioral health information in a manner that is easy to use and enables them to make choices about disclosure of specific information that is sensitive to the individual and/or legally protected.	3. Call to action: Individuals should be able to trust that their health information (such as that generated/collected via home monitoring devices or other emerging technologies) is protected and secure.	4. ONC and the industry will continue to provide individuals with relevant and updated resources based on current technology to assist with increasing their digital health literacy.

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
C4. Education and digital health literacy for individuals	1. Call to action: Consumer advocacy groups in collaboration with government agencies, associations and payers should develop and disseminate resources (toolkits and best practices) based on consumer needs to assist individuals with increasing their digital health literacy. This supports consumer participation in shared decision-making with their care team based on more complete and accurate information.	2. ONC, government and the industry should work with individuals to help the majority understand the value of health IT for managing their health by providing individuals with easy resources to assist with increasing their digital health literacy. 3. ONC and the industry should continue to provide individuals with relevant and updated resources based on current technology to assist with increasing their digital health literacy.	4. ONC and the industry should work with individuals to ensure that a majority understand the value of sustained engagement in managing their health, supported by health IT. 5. ONC and the industry should continue to provide individuals with relevant and updated resources based on current technology to assist with increasing their digital health literacy.

Care Providers Partner with Individuals to Deliver High Value Care

LHS Requirement

D. ***Care providers partner with individuals to deliver high value care:*** Providers share and use information from multiple sources as they transform the way they provide care and engage with patients to routinely assess and incorporate patient preferences and goals into care plans that achieve measurable value for individuals and the population.

<div>

FEDERAL HEALTH IT STRATEGIC PLAN OBJECTIVES SUPPORTED

▸ Protect and promote public health and healthy, resilient communities
▸ Empower individual, family and caregiver health management and engagement
▸ Improve clinical and community services and population health
▸ Support the delivery of high-value health care
▸ Improve health care quality, access and experience through safe, timely, effective, efficient, equitable and person-centered care

</div>

Background and Current State

In partnership with individuals, their families and caregivers, health care providers and provider organizations are central to the delivery of high quality, safe and efficient health care. Providers[33] are not only stewards of the majority of clinical health information today, but they jointly make decisions with individuals about diagnosis and treatment and play a critical role in coordinating care with other providers to support patients. Rigorous training, continuing education and maintenance of certification programs, coupled with decades of advancement and innovation in health care have earned providers the trust of the American public. Most importantly, the profound and fundamental nature of the patient-provider relationship sets the profession of medicine apart from most others and has earned its practitioners the honor of participating in many of the most important events and decisions that individuals and families face.

Many provider communities have recognized that team-based care, strong care coordination and effective patient engagement are fundamental to an efficient care delivery system. However, coordinating care and engaging with multi-disciplinary, cross-organization care teams has been incredibly difficult with the tools available today. Technology that does not make it easy to share and use the electronic health information that providers need, when they need it, often creates additional challenges to care coordination.

Moving Forward and Critical Actions

This Roadmap shifts the nation's focus from meaningfully using specific technologies with specific features to working together as a nation to achieve the outcomes desired from interoperability and a learning health system. Providers should have the tools they need to support a cultural shift in the way they practice medicine and use technology that supports the critical role of information sharing. The shift will open up new possibilities for providers in how they engage with patients, how they interact with other care team members and brings with it significant opportunities for progress and innovation.

For example, the availability of holistic longitudinal information on each individual in a computable format will enable significant advancements in the quality of care through more rapid and efficient cycles of improvement, using clinical decision support (CDS) tools. Additionally, based on the adage that one cannot fix what one cannot measure, the expansion of data availability to include data from a variety of relevant sources in the calculation of electronically specified clinical quality measures (eCQMs) will be important to guiding the transformation of the delivery system to a learning health system.

---

[33] For purposes of this Roadmap, the term care providers is broadly inclusive of the care continuum and includes individuals and organizations that hold professional licenses and certifications that grant them permission to play a role in the treatment of individuals as part of a community. This includes providers such as primary care physicians, specialists, nurses, physical therapists, pharmacists, dentists, social workers, optometrists and other allied health professionals, as well as organizations such as hospitals, public health departments, mental health and substance abuse services, long- term and post-acute care facilities, home and community-based services, other support service providers, care managers and other authorized individuals and institutions.

In a learning health system, data will be created and collected automatically during the routine provision of care, alleviating the need for duplicate entry of data into registries and other parallel systems. This data will not only seamlessly enable improvement in the quality of care but also, as enabled by individual permission, will support secondary uses of data that help to achieve important advances in population health management, public health and the generation of new biomedical knowledge. Close integration of CDS into health IT systems will enable the rapid dissemination of new knowledge to support the use of best evidence in the care of all patients, including those with multiple, complex or rare conditions.

For example, CDS based on wide availability of pharmacy prescribing and fill data will enable patient education, prevention of adverse drug events, tracking and improvement of medication adherence and, through linkages to Prescription Drug Monitoring Program (PDMP) systems, enable interventions to prevent the abuse of controlled substances. Further, the integration and wide availability of this information will support distributed models of care management, comprehensive medication management (CMM) and medication therapy management (MTM) across multiple healthcare disciplines and sites of care, such as community pharmacies. See Appendix F for more Background information on Medication Use and Management.

In a learning health system, integrated cost and quality data will be widely available to all stakeholders. Providers will use cost and quality data to help patients choose their preferred treatments. Consistent information on health care outcomes and transparency of health costs will assist individuals in making care decisions; providers in improving care; and purchasers in moving from pay for volume to pay for value. This will require standards improvements, policy changes, coordinated governance and infrastructure investment.

With the availability and appropriate presentation of holistic, longitudinal health information, accurate outcome measures, especially patient-reported outcomes, will support innovation of care models, allow providers to customize workflows and support research. With these measures consistently available throughout the health system, new interventions can be studied with minimal investment and comparative effectiveness information will be available for all therapeutic options.

A continuous cycle of improvement will emerge, in which information gathered and decisions made during the normal course of care will be transformed in real-time into computable data and knowledge that will inform clinical decisions, report on notifiable conditions or events, measure quality of care and provide evidence for patient-centered outcomes research. This rapid and actionable feedback, when implemented in care delivery workflows optimized for usability, safety, quality and respect for patient preferences, will continuously improve the interactions and decisions of providers, care teams and patients/individuals.

Table 4: Critical Actions for Care Providers Partner with Individuals to Deliver High Value Care

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
D1. Organization/ Governance	1. Call to action: Providers should participate in governance of interoperability at all levels, from regional efforts to nationwide coordinated governance.	2. Call to action: Providers should continue to provide input on the evolution of coordinated governance to support a learning health system.	3. Call to action: Providers should remain active in coordinated governance.
D2. Providers embrace a Culture of Interoperability and work with vendors and other supporting entities to improve interoperability	1. Call to action: Providers should routinely expect electronic access to outside information in the provision of care and engage with other providers to send, receive, find and use health information for their patients. 2. Call to action: Providers should recognize that valuable clinical information about their patients may reside with patients or caregivers themselves and that they may need to incorporate that information into their decision making. 3. Call to action: Providers and their organizations should embrace the use of enabling technologies such as publish/subscribe and query-based exchange with single sign-on to minimize workflow barriers to interoperability. 4. Call to action: Providers and their organizations should ensure contracts and agreements that they sign and re-sign with technology developers include necessary requirements for interoperability, to ensure they can share and incorporate patient information	5. Call to action: Providers should routinely access and use health information from other sources, including individuals, when making clinical decisions 6. Call to action: Providers should routinely populate key data when E-prescribing in support of unambiguous prescription for verification, counseling, monitoring and activities of comprehensive medication management. 7. Call to action: Providers and their organizations should work with necessary parties to configure systems to alert providers to the presence of relevant information from other sources and make it conveniently available to the provider. 8. Call to action: Providers and their organizations should work with necessary parties to configure systems so that the presentation of information to providers is configurable based on use case, provider specialty and other characteristics, to facilitate usability and patient safety.	9. Call to action: Providers should practice in a new way, with a new culture of electronic health information sharing, access and use for both clinicians and institutions is firmly established. 10. Call to action: Providers should routinely use and have access to robust and clinically relevant decision support (e.g. for medication management). 11. Call to action: Providers should regularly use and have access to the most relevant, integrated information, appropriate notifications. 12. Call to action: Providers should receive and provide continuous feedback to support the improvement of decision-making, care processes and outcomes. 13. Call to action: Providers should use new evidence-based guidelines and tools for care that are disseminated rapidly to providers through decision support and other timely and context-sensitive pathways.

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
D3. Accurate Measurement	1. Call to action: Providers should leverage data beyond their internal systems for population health analytics and quality measurement (eCQMs) including supporting value-based payment models.	2. Call to action: Providers and other stakeholders should use standard metrics of interoperability to monitor and track improvement. 3. Call to action: Providers and other stakeholders should use standard metrics for interoperability and health outcomes to improve clinical care and processes. 4. Call to action: Providers should be able to report on measures based on the most representative data available about each patient.	5. Call to action: Public and private stakeholders should objectively measure and value interoperability and information sharing as an indicator of care coordination, quality and efficiency. 6. Call to action: Providers should be able to report on measures based on more complete and consistent representative data about each patient.

D4. Interoperability of processes and workflows	1. Call to action: Providers should routinely leverage standards-based health IT to support prioritized workflows including:
	  o Closed loop transitions of care
	  o Secure clinical communications
	  o Prior authorizations, medication co-pays and imaging appropriateness
	  o CPOE for services and diagnostic testing
	  o e-prescribing of controlled substances with concurrent availability of PDMP data
		2. Call to action: Providers should engage with an expanded set of interoperable workflows, including:
		  o Plug-and-play clinical decision support services
		  o Electronic consultations
		  o Reporting to specialty society registries
		  o Reporting to value-based payment programs
		  o e-prescribing supported by complete medication fill history
		  o Discovery and incorporation of information from patient-owned devices with tools for reconciliation and validation
		  o Recommendation of patients to relevant studies and trials
		  o Exchange of information to support comprehensive medication management and MTM services
			3. Call to action: Providers should leverage a robust library of interoperable workflows to support care processes across the continuum of care, including tools for integration, reconciliation and validation of external information.

D5. Training and maintenance of certification for providers	1. Call to action: Public and private stakeholders should incorporate interoperability into the training of new providers and continuing professional education. 2. Call to action: Professional specialty boards and other certifying bodies should agree on standards for interoperable registries and maintenance of certification.	3. Call to action: Public and private stakeholders should agree on a way in which to measure progress and competency of trainees is evaluated and scored using interoperable, standards based clinical information. 4. Call to action: Professional specialty boards and other certifying bodies should receive most of the information required from their diplomats through information exchanged in a standard format. 5. Call to action: Professional specialty boards should utilize standardized electronic data and formats to populate registries.	

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
D6. Innovation and Generation of New Knowledge and Evidence	1. Call to action: Providers currently engaged in clinical research and quality improvement should work together with research institutions and other public and private stakeholders to establish a strategic plan for research and the generation of new knowledge.	2. Call to action: Providers should further engage with the research community and should routinely offer patients and families participation in research and quality improvement programs. 3. Call to action: Community or region-wide Institutional Review Boards should ensure that the appropriate patient protections are in place to conduct multi-sourced clinical research.	4. Call to action: Researchers, providers and other stakeholders should accelerate and measure the pace of innovation and research, as well as the dissemination of new knowledge to improve health and care. 5. Call to action: Technology developers should enable patient-centered and future clinical research methods for accelerated deployment of research findings into clinical care.

D7. Transparency of Value and engagement of patients, families, and caregivers	1. Call to action: Providers should work together with purchasers of care to have access to patient out-of-pocket costs and those of payers and purchasers. Providers are engaged in regional efforts to measure quality and maximize value.
	2. Call to action: Providers should offer and encourage access to medical records and secure communications with all patients and any family and caregivers who are authorized to engage in such communications.
	3. Call to action: Providers should support consumers in downloading or transmitting their health information to a destination of their choice.
		4. Call to action: Providers should routinely utilize cost and quality data to make shared diagnostic and treatment planning decisions.
		5. Call to action: Providers should work together with purchasers of care to develop, test and implement appropriate and credible indicators of value.
		6. Call to action: Providers should support consumer-facing services such as:
		  o Online scheduling
		  o Medication refill requests
		  o Electronic/Telehealth Visits
		  o Patient provided device data, screenings and assessments
		  o Informed consent and education modules
		  o Integration of patient-generated health data in the medical record
		  o Patient-defined goals of care
		  o Shared care planning
			7. Call to action: Providers should demonstrate the value of their care to those who receive and pay for it using objective, trusted metrics.
			8. Call to action: Providers and individuals should work together to substantially reduce the burden of care coordination through patient-centered tools and sharing and use of electronic health information.
			9. Call to action: Individuals should interact easily and seamlessly with their care team as they transition into and out of the health care system, communicating remotely with their care team as needed over time, rather than only in face-to-face care situations.

Privacy and Security Protections for Health Information

Participation in and use of a learning health system will be highly dependent upon reliable mechanisms to ensure that (1) a secure network infrastructure is widely available; (2) privacy is protected; (3) health information and services are accessed only by participants whose identity has been verified and who have been authenticated to access the system they are seeking to access; (4) users have access only to data they are authorized to access, where authorization is determined by individuals' choices, or, if no choices are recorded, what the statutes, regulations and consensus rules say a user may access, use, disclose and receive. All of these components are necessary for enabling broad scale interoperability and a learning health system.

Ubiquitous, Secure Network Infrastructure

LHS Requirement

E. *Ubiquitous, secure network infrastructure:* Enabling an interoperable, learning health system requires a stable, secure, widely available network capability that supports vendor-neutral protocols and a wide variety of core services.

FEDERAL HEALTH IT STRATEGIC PLAN OBJECTIVES SUPPORTED

▸ Advance a national communications infrastructure that supports health, safety and care delivery
▸ Protect the privacy and security of health information
▸ Increase access to and usability of high-quality electronic health information and services

---

Background and Current State

Security of the network infrastructure is pivotal to ensuring success of a learning health system. It is the basis for enabling necessary trust that data can be shared in a way that keeps it secure and private, unaltered in an unauthorized or unintended way and available when needed by those authorized to access it. There are a number of components that will ultimately enable a ubiquitous, secure network infrastructure, including cybersecurity and encryption. Additionally, in a learning health system, the security of the systems and their underlying security infrastructure will continuously evolve as necessary to maintain its secure state.

As health IT systems have become increasingly connected to each other, cyber threats have concurrently increased at a significant rate. In an interoperable, interconnected health system, an intrusion in one system could allow intrusions in multiple other systems. Additionally, there is high variability in the capabilities and resources healthcare organizations have at their disposal to prevent cyber-attacks. Large organizations have the resources and expertise to have a dedicated information security team to address cybersecurity; however, small and mid-sized health care organizations, like other small businesses, may not have these resources and may not be able to afford them. Finally, there is a significant behavioral and cultural change necessary in the industry regarding the relevance of

cybersecurity risks. Many in the industry do not realize the significant risk to their systems and do not understand the importance and urgency of implementing security best practices to prevent cyber-attacks. Despite being identified as critical infrastructure for the nation, the healthcare system could do more to prepare for a cyber-security attack.[34]

Encryption of data is a second component of a ubiquitous, secure network infrastructure. Encryption is a method of scrambling or encoding data, so that it cannot be read without the appropriate key to unscramble the content. Encryption is applied when data is sent (particularly over networks that are not secure otherwise, like the Internet) and when it is stored. These are sometimes referred to as information in transit and information at rest, respectively. In both cases, the core mechanism is the same. A software program takes a piece of information (a string of data bytes) and changes it into another piece of information (a different string of bytes, not necessarily the same number of bytes). For encryption to work, it must be possible for another program (or possibly another algorithm in the same program) to reverse the process and change the encrypted information back into the information in the clear. This is called decrypting. Another constraint is that the algorithm to decrypt should itself be secure; otherwise, unwanted recipients would be able to recover the original information.

Encryption is a safe harbor provision under the Breach Notification Rule.[35,36] This means that if a HIPAA Covered Entity (CE) or Business Associate (BA) (who may have custody of the protected health information or PHI), such as a cloud-based EHR and data services provider, chooses to encrypt PHI consistent with guidance in the Breach Notification Interim Final Rule, 74 Fed. Reg. 42740 (Aug. 24, 2009) and discovers a breach of that encrypted information, neither a CE nor a BA is required to provide the breach notifications specified under the Rule. See Appendix C for more information on cybersecurity and encryption.

Moving Forward and Critical Actions

A learning health system's cybersecurity program encompasses, but is not limited to, the following:

- Contracts, such as Data Use Agreement, Memorandum of Understanding/Memorandum of Agreement (MOU/MOA), Interconnection Security Agreement (ISA), and Business Associate Agreement (BAA). These documents, which are typically bi-lateral between two parties, exist in addition to each party's own compliance documents such as HIPAA Privacy & Security Policies and Procedures, or other documents required by law. Collectively, the bilateral documents *and* the individual organization's policy and compliance documents document the regulatory and other requirements for security controls, technical implementation as well as business to business requirements for connecting between health IT systems;

---

[34] http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf

[35] 45 CFR 164.404(a). October 2011. http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-404.pdf

[36] 74 FR 42740 pg. 42742. August 2009. http://www.gpo.gov/fdsys/pkg/FR-2009-08-24/pdf/E9-20169.pdf

- Cross-organizational threat information sharing and mature incident response capabilities;
- Incident Management and Response policies and procedures are in place and a response team is identified within the organization;
- The functional contents of all network messages are fully encrypted; and,
- All data stored in any database connected to the network (whether through a companion system, interface engine, or gateway) is fully encrypted.

Table 5: Critical Actions for Ubiquitous, Secure Network Infrastructure

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
E1. Cybersecurity	1. ONC will work with OCR to release an updated Security Risk Assessment tool and hold appropriate educational and outreach programs. 2. ONC will coordinate with the Office of the Assistant Secretary for Preparedness and Response (ASPR) on priority issues related to cyber security for critical public health infrastructure. 3. HHS will continue to support, promote and enhance the establishment of a single health and public health cybersecurity Information Sharing and Analysis Center (ISAC) for bi-directional information sharing about cyber threats and vulnerabilities between private health care industry and the federal government. 4. ONC will work with NIST and OCR to finalize and publish the NIST Critical Infrastructure Cybersecurity Framework and Health Insurance Portability and Accountability Act (HIPAA) Security Rule Crosswalk. 5. HHS will work with the industry to develop and propose a uniform approach to enforcing cybersecurity in healthcare in concert with enforcement of HIPAA Rules.	6. Stakeholder input requested	7. Stakeholder input requested
E2. Encryption	1. ONC will work with OCR and industry organizations to develop "at rest" standards for data encryption and provide technical assistance. OCR will consider whether additional guidance or rulemaking is necessary. 2. ONC will work with OCR and industry organizations to develop "in transit" standards for data encryption and provide technical assistance. OCR will consider whether additional guidance or rulemaking is necessary. 3. ONC will develop guidance for implementing encryption policies. 4. ONC will work with payers to explore the availability of private sector financial incentives to increase the rate of encrypting, starting with discussions with casualty insurance carriers who offer cybersecurity insurance.	5. Stakeholder input requested	6. Stakeholder input requested

Verifiable Identity and Authentication of All Participants

LHS Requirement

F. ***Verifiable identity and authentication of all participants****:* Legal requirements and cultural norms dictate that participants be known, so that access to data and services is appropriate. This is a requirement for all participants in a learning health system regardless of role (individual/patient, provider, technician, etc.)

FEDERAL HEALTH IT STRATEGIC PLAN OBJECTIVES SUPPORTED

‣ Protect the privacy and security of health information

Background and Current State

Legal requirements and cultural norms dictate that the identity of participants who are accessing electronic health information be known so that access to data and services is appropriate. A learning health system will require that all participants, regardless of role (e.g., patient, provider, researcher), be identified and authenticated so that there is a high level of trust that participants are who they say they are and participants cannot fraudulently pose as someone else. Without appropriate identification and authentication policies, processes and technologies, individuals will not trust that their health information and other data are secure and private.

The HIPAA Security Rule establishes national standards to protect individuals' electronic protected health information (PHI). PHI is defined as personal health information that is created, received, used, or maintained by a covered entity or business associate. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic PHI. These safeguards are designed to prevent unauthorized or inappropriate access, alteration, use, or disclosure. The Security Rule also includes a Person or Entity Authentication Standard,[37] which requires covered entities to implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed. However, the Security Rule does not specify authentication options, assurance levels, or verification requirements, as entities are to determine themselves what is appropriate in their particular environments. The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164.

Identity proofing is the process of verifying that a person is who he says he is through representative identifiers, usually for the purpose of assigning a credential that carries a token (*e.g.,* password or certificate pin) to be used later by the individual to access an information system. Identity proofing of providers and patients is necessary for a number of purposes. From the provider's perspective, it could include accessing the EHR at their hospital or practice, sending an electronic prescription, accessing a

---

[37] 164.312(d)

health information organization's query portal, or sending secure messages (whether Direct messages or other types of secure messages). For a patient, it could be accessing their health information from a patient portal. The identity proofing process requires the participant to present supporting documentation for verification. In general, two forms of identification are required and at least one of those must be a government issued form of identification (*e.g.,* driver's license, passport, etc.). Additional forms of identification, such as a utility bill, financial record, or the patient's health plan card, are often accepted. The level of verification ranges widely from visually inspecting and photocopying what was presented to contacting the source of the information during the registration process.

Authentication is the process of establishing confidence in the identity presented to gain access to a system. Authentication sometimes utilizes tokens (also called factors for authentication) that a participant provides to demonstrate they are the person who should have access. Tokens can be something a participant knows (a password), something a participant has (ID badge or hardware token/fob), or something a participant is (typically a biometric like a fingerprint). Depending on the risks of authentication errors, one or more factors may be required for authentication.

Federal agencies are required to adhere to OMB M-04-04, E-Authentication Guidance for Federal Agencies. OMB M-04-04 defines four levels of assurance (LOA) as a means to weigh the risks associated with authentication errors and misuse of credentials. Level 1 is the lowest assurance level (little or no effect) and Level 4 is the highest (may cause great harm). The NIST document SP 800-63-2 provides technical guidance that includes the identity proofing process and all aspects of credential management based on the OMB M-040-04 weight scale. While federal agencies require specific LOAs for their own use cases and while other industries have standard LOA requirements for their sector's cybersecurity, the health care industry has not standardized its LOA requirements for identity proofing and authentication.

The lack of consistently applied methods and criteria for both identity proofing and authentication has significantly hampered the exchange of data across organizations. For example, Direct was intended to work much like email and lower the barrier for exchange for providers and hospitals by eliminating the need for complex legal agreements between individual organizations. However, many health information service providers (HISPs) have different identity proofing and authentication policies and requirements. Or, HISPs may not acknowledge the identity proofing and authentication undertaken upstream by another organization. This variation has led to the creation of multiple trust organizations and individual agreements between organizations. Ultimately, providers and hospitals are limited to exchanging data only with those individuals or organizations with whom they (or their HISP) have created an agreement. In a learning health system, in contrast, the providers and hospitals should exchange with any other provider or hospital appropriately identity proofed and authenticated and especially with providers or hospitals that a patient directs them to share with.

The ONC HIT Policy Committee (HITPC) has put significant effort into recommendations to ONC for addressing both provider and patient identity proofing and authentication issues over the last three years. Its recommendations recognize that multi-factor authentication is feasible and is consistent with the direction the industry is headed, just like other industries with more mature information

infrastructures. Additionally, HITPC's recommendations have strongly encouraged providers to use multi-factor authentication for provider remote access to PHI and for patient access to patient portals. The HITPC did not give any specific requirements for identity proofing beyond support of the existing HIPAA Security Rule guidance, but did encourage ONC to disseminate and distribute best practices for identity proofing and authentication.[38]

In 2010, the National Strategy for Trusted Identities in Cyberspace (NSTIC) was launched as a public-private collaborative to help, "individuals and organizations utilize secure, efficient, easy-to-use and interoperable identity credentials to access online services in a manner that promotes confidence, privacy, choice and innovation."[39] NSTIC has worked over the last few years to develop pilots to test various electronic means for ensuring identity and authenticating users and ultimately develop an identity ecosystem that can be utilized to mitigate cybersecurity issues and maintain the privacy of individuals. Based on the NSTIC's work, as well as wide agreement across various sectors (financial, health, defense, etc.), multi-factor authentication and solid identity proofing processes have been acknowledged as the new norm. A recent Executive Order also pushes for alignment with NSTIC.[40]

Moving Forward

The use of mobile phones, email and other factors for authentication has become commonplace in many sectors such as banking and e-commerce. With the emergence of Internet accessible medical devices, monitors and the yet-to-be-developed Internet of Things,[41] it is not too far-fetched to imagine a time in the near future in which a mobile device may be used to identity proof and authenticate a patient and their associated devices at the point of care. This in turn could serve to promote a person-centric environment that would minimize the need for intermediaries to facilitate trust.

To prepare, the nation can take some simple steps to pave the way today: establish common identity proofing practices at the point of care; require multi-factor authentication for all patient and provider access to health IT systems in a way that aligns with what is required in other industries; leverage existing mobile technologies and smart phones to provide efficient, effective paths for patient or provider identity authentication; and integrate the RESTful approaches to authentication in anticipation of that vision of tomorrow.

---

[38] http://www.healthit.gov/facas/health-it-policy-committee/health-it-policy-committee-recommendations-national-coordinator-health-it

[39] http://www.nist.gov/nstic/index.html

[40] Improving the Security of Consumer Financial Transactions. October 17, 2014. http://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions

[41] The Internet of Things (IoT) refers to the connection of a wide variety of uniquely identifiable devices across the existing Internet infrastructure (e.g., smart phones, wearable and implantable devices, etc.).

Table 6: Critical Actions for Verifiable Identity and Authentication of All Participants

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
F1. Policies and Best Practices	1. Policies established through the coordinated governance process will adopt the concept of multi-factor authentication for all roles that access health information, subject to contextual appropriateness and consistency with the HIPAA Security Rule.[42] 2. ONC will identify and undertake (where necessary) work to harmonize other standards with those adopted for multi-factor authentication. 3. Through coordinated governance, stakeholders (with input from OCR) will establish and adopt best practices for identity proofing that are consistent with standards already adopted for other, comparable industries and with the HIPAA Security Rule.	4. Stakeholder input requested	5. Stakeholder input requested
F2. Standards	1. Health IT developers will leverage existing mobile technologies and smart phones to provide efficient, effective paths for patient or provider identity authentication. 2. SDOs will work with health IT developers to conduct Pilots using RESTful approaches for authentication.	3. Stakeholder input requested	4. Stakeholder input requested

---

[42] In September 2012 and May 2013, the HITPC recommended to the ONC that multi-factor authentication be utilized for providers and patients respectively. In October 2014, an Executive Order required National Security Council staff, the Office of Science and Technology Policy and OMB to draft a plan for ensuring "that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate."

Consistent Representation of Permission to Collect, Share and Use Identifiable Health Information

LHS Requirement

G. ***Consistent representation of permission to collect, share and use identifiable health information***: Though legal requirements differ across the states, nationwide interoperability requires a consistent way to represent an individual's permission to collect, share and use their individually identifiable health information, including with whom and for what purpose(s).

FEDERAL HEALTH IT STRATEGIC PLAN OBJECTIVES SUPPORTED

▸ Protect the privacy and security of health information

Background and Current State

The success of health IT and interoperability is dependent on individuals' trust that their health information will be kept private and secure and that their rights with respect to this information will be respected.[43] The parameters of individual choice regarding collection, sharing and use of an individual's health information are defined across three broad categories that impact interoperability: statutes and regulations, organizational policy and technology. Statutes and regulations include federal and state laws and regulations that set individual privacy protections for health information. Laws and regulations serve three purposes: First, they specify requirements of data holders to protect a person's individually identifiable health information. Second, they specify the conditions under which an individual's health information can be accessed, used and disclosed with or without the individual or his/her representative's explicit authorization. Third, they specify the purposes or conditions under which an individual's information can be accessed, used, or disclosed only with the individual or their representative's express authorization.

HIPAA and its implementing regulations set a national baseline of federal health information privacy and security protections. The HIPAA Rules create requirements that health plans, most health care providers and health care clearinghouses, as well as their business associates, must follow. The HIPAA Rules also provide rights for individuals to obtain access to their PHI and rules governing when protected health information may be used or disclosed without individual's express authorization. A number of other current federal and state health information privacy laws and regulations exist that have heightened privacy protections and require documented, individual choice to share certain types of health information. Some examples of federal regulations that contain these special protections are the Federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations (42 U.S.C. § 290dd-2) that

---

[43] http://www.hhs.gov/strategic-plan/patient-privacy.html

apply to behavioral health treatment information[44] and federal laws (38 USC § 7332) protecting certain types of health information coming from covered U.S. Department of Veterans Affairs facilities and programs.[45]

Many states have laws and regulations to protect the privacy of health information that have stricter privacy protections and requirements on use and disclosure than the HIPAA Rules. These laws and regulations vary from state-to-state, often narrowly targeting a particular population, health condition, data collection effort or specific types of health care organizations. As a result, states have created a "patchwork" of health information privacy laws and protections that address individual choice and are not uniform across state lines or care settings/encounters. This patchwork is also not easily understood by individuals.

Organizational policies are organization-level rules regarding individual choice for use and disclosure of health information (within the bounds of state and federal regulations). Organizational policies vary even within single states and create an additional layer of differing approaches and parameters for individual choice. Unlike laws, organizational policies may be and often are, developed within a specific organization and therefore are not typically subject to public debate or public consensus building. Moreover, organizational policies often include requirements not specifically mandated by law.

Technological advances are creating opportunities to share data and allow patient preferences to electronically persist through an interoperable learning health system. Technology provides a means for electronically identifying, capturing, tracking, managing and communicating an individual's choice preferences regarding the use and disclosure of health information from the originating source to other technical systems. Health IT enables not only the capture of a documented choice, but also the capture of what permissions apply, even when there is no documented choice. Health IT can enable users to comply with relevant use and disclosure laws, regulations and policies in an electronic health information environment. (See Appendix D for deeper background on these three categories.)

Fair Information Practice Principles[46]

Adoption and effective implementation of privacy protections is essential to establishing the public trust necessary for broad scale interoperability of health information. The Fair Information Practice Principles (FIPPs) are a common set of overarching principles that guide information practices while advancing

---

[44] http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=02b3d31742318b503b8d4ba0111d0e35&tpl=/ecfrbrowse/Title42/42cfr2_main_02.tpl

[45] http://www.gpo.gov/fdsys/pkg/USCODE-2011-title38/pdf/USCODE-2011-title38-partV-chap73-subchapIII-sec7332.pdf

[46] In 1973, the Department of Health, Education and Welfare (HEW) released its report, Records, Computers and the Rights of Citizens, which outlined a Code of Fair Information Practices that would create "safeguard requirements" for certain "automated personal data systems" maintained by the Federal Government. This Code of Fair Information Practices is now commonly referred to as fair information practice principles (FIPPs). See Department of Health, Education and Welfare, *Records Computers and the Rights of Citizens* (July 1973), available at http://www.justice.gov/opcl/docs/rec-com-rights.pdf.

technology. They are foundational to many laws, regulations and policies in the public and private sector, including the HIPAA Privacy Rule, the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information and many state laws and organization-level policies.[47] So too, this roadmap uses the FIPPS as a touchstone for building a privacy and security framework for interoperability. The Nationwide Privacy and Security Framework (based on the FIPPs) are specific objectives identified by ONC in earlier work. Proposals below reference these principles.

The FIPPs identify that individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their individually identifiable health information (choice) and that individuals need to understand their choice and how their data is used. In an interoperable learning health system, that means there must be both policies and technology that:

1. Provide individuals the opportunity to make meaningful decisions about their health information;
2. Capture information about choice in a manner that can be communicated and recognized across a broad ecosystem of technology;
3. Represent choice in a consistent manner so that it can be appropriately acted upon (ideally over time, in automated ways between technical systems);
4. Enable providers to deliver health care to individuals using appropriately exchanged electronic health information even when the individual has not stated a preference; and
5. Allow individuals, especially those who have not stated a choice, to understand how the information system works, especially for number four above.

---

[47] There are many versions of the FIPPs; the ONC FIPPs are in the Nationwide Privacy and Security Framework for Electronic Health Information Exchange ("Nationwide Privacy and Security Framework") released in 2008: http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf. In 2012, ONC issued privacy and security guidance to the state health information exchange cooperative agreement program that is based on the Nationwide Privacy and Security Framework for Electronic Health Information Exchange. See ONC's State Health Information Exchange Program Instruction Notice (PIN), Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program, March 2012, http://www.healthit.gov/sites/default/files/hie-interoperability/onc-hie-pin-003-final.pdf.

Nationwide Privacy and Security Framework (based on the FIPPs)

1. **INDIVIDUAL ACCESS:** Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.
2. **CORRECTION:** Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information and to have erroneous information corrected or to have a dispute documented if their requests are denied.
3. **OPENNESS AND TRANSPARENCY:** There should be openness and transparency about policies, procedures and technologies that directly affect individuals and/or their individually identifiable health information.
4. **INDIVIDUAL CHOICE:** Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their individually identifiable health information.
5. **COLLECTION, USE, AND DISCLOSURE LIMITATION:** Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.
6. **DATA QUALITY AND INTEGRITY:** Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.
7. **SAFEGUARDS:** Individually identifiable health information should be protected with reasonable administrative, technical and physical safeguards to ensure its confidentiality, integrity and availability and to prevent unauthorized or inappropriate access, use, or disclosure.
8. **ACCOUNTABILITY:** These principles should be implemented and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

SOURCE: http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf

---

Basic Choice v. Granular Choice

"Basic choice" is the choice an individual makes about the use and disclosure of their health information generally, including electronic exchange of health information that is not subject to heightened use and disclosure restrictions under state or federal law. HIPAA rules permit the use and disclosure of PHI for, among other purposes, treatment, payment and health care operations of a HIPAA covered entity (TPO) without an individual's express permission (often called "consent"). Nevertheless, many health care organizations still choose to obtain an individual's written permission for use and disclosure of PHI for TPO.[48] This type of consent activity represents "basic choice."[49] Basic choice builds on existing standards

---

[48] For more information about health information privacy law pertaining to individual choice, see ONC's Meaningful Choice Resource Center, http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/health-information-privacy-law-policy.

HIPAA Privacy Rule standards of "minimum necessary," [50] "role based access," and use of de-identification when possible.[51] Basic choice" does not refer to circumstances where special legal requirements about identified clinical conditions apply; for the purposes of the Roadmap, those are treated under the concept of "granular choice."

"Granular choice" refers to the choice an individual makes to share specific types of information, including (1) information that fits into categories to which, by law, protections in addition to HIPAA apply; (2) the choice afforded an individual based on their age; and (3) the choice to share health information by specific provider or payer types. Many stakeholders believe, and several laws reinforce, that individuals should have the ability to control use and disclosure of specific health information, or to specify which providers may have electronic access to it. For example, the results of a nationwide ONC survey on consumer attitudes found that when their health information is exchanged electronically, nearly all respondents (about 92%) want to be able to share only portions of their medical records with others.[52]

This is consistent with the individual choice principle in FIPPs. One example is federal law (e.g., 42 U.S.C. § 290dd-2), which requires health care providers to obtain patients' written consent before they disclose information about a patient's substance abuse treatment to other people and organizations, even for treatment. Granular choice refers, therefore, not only to granular choice among clinical conditions that are protected by laws in addition to HIPAA, but eventually, granular choice, should a patient wish to express it, regarding other data distinctions to be determined, but which are consistent with a learning health system, such as research purposes in which an individual has chosen to participate.

Moving Forward

The U.S. legal, regulatory and policy landscape for sharing health information is complex. While the laws are designed to protect health information and individual rights, they also must enable appropriate

---

[49] The National Governors Association has published a landscape analysis of these laws that concern whether the patient wants to allow any of their information to be exchanged, the oft-called "opt in/opt out." http://www.nga.org/files/live/sites/NGA/files/pdf/1103HIECONSENTLAWSREPORT.PDF; see also RTI International prepared for ONC, *Report on State Law Requirements for Patient Permission to Disclose Health Information*, August 2009, http://www.healthit.gov/sites/default/files/disclosure-report-1.pdf.

[50] 45 CFR 164.502(b), 164.514(d)

[51] U.S. Department of Health and Human Services, Office for Civil Rights, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html

[52] U.S. Department of Health and Human Services, Office of the National Coordinator, Health Information Security and Privacy Collaboration: Survey of Attitudes toward Electronic health Information Exchange and Associated Privacy and Security Aspects, (Wash. D.C.: January 2011), http://www.healthit.gov/policy-researchers-implementers/health-information-security-privacy-collaboration-hispc. The survey used the term "privacy settings," defined as allowing permission for some portions of an individual's health records to be shareable and other portions to not authorized to be accessed, used, or disclosed.

information sharing to support health and health care. Despite efforts to address potential technology standards and solutions for individual choice across this complex ecosystem, it has become clear that the complexity of the rules environment will continue to hinder the development and adoption of a consistent nationwide technical framework (e.g., data elements, definitions, vocabularies) for electronically managing individuals' basic and granular choices until the complexity is resolved.[53] Reducing variation in the current legal, regulatory and organizational policy environment related to privacy that is additive to HIPAA will help facilitate the development of technical standards and technology that can adjudicate and honor basic and granular choices nationwide in all care settings, while ensuring that special protections that apply as a result of deliberative legislative processes remain conceptually in place. Through the course of harmonization, however, individual privacy rights as specified in state and federal laws must not be substantively eroded. For example, where a law protects reproductive health or behavioral health information (to name but two sensitive conditions), harmonization would not mean the substantive weakening of such protections.

Consistent with the governance principle of individual choice outlined elsewhere in this Roadmap, HHS is committed to encouraging the development and use of organizational policy and technology to advance individuals' rights to make choices about the use and disclosure of their electronic health information. HHS also supports the development of standards and technology to facilitate individuals' ability to control the disclosure of specific information that is considered by many to be sensitive in nature (such as information related to substance abuse treatment, reproductive health, mental health, domestic or sexual violence, or HIV/AIDS) in an electronic environment.[54]

Methods to consistently capture, communicate and automate processing of individual choice will be essential as additional systems and stakeholders are interoperable. These same automated processes are essential to support clinical research, population health and public health. Both an individual's "basic choice" and "granular choice" will also need to persist as data is shared from the point of origin to each subsequent system.

To ensure consistent technical representation of an individual's choice regarding use and disclosure of their health information across the learning health system, the nation will need to make aggressive progress to understand, align and harmonize laws and organizational policy so that individuals can more fully understand how data about them is being used (consistent with FIPPs.) In particular, the following three areas of policy will require attention before addressing technology standards to capture, communicate and process individual choice across the learning health system:

1. **Exchange permitted for certain purposes without an individual's written permission.** Working to help all stakeholders understand the protections of existing laws will establish a clear foundation for the public's understanding and expectations for how most PHI (that does not

---

[53] http://www.healthit.gov/facas/calendar/2014/12/17/standards-transport-security-standards-workgroup

[54] Excerpt from HHS Secretary Strategic Initiative focused on Privacy. March 2014: http://www.hhs.gov/strategic-plan/patient-privacy.html

have applicable special legal protections) can be used and disclosed (including through electronic exchange), if an individual takes no action to document a basic choice, no matter where an individual or their health information resides.

2. **Individuals understand their basic choice:** Individuals understand how their information is being moved (exchanged) for TPO (as primary uses), what their choices are for "basic choice" (choice regarding electronic exchange) and how their information will be protected, used, or disclosed even if the individual makes no active choice.

Standardize the meaning of sensitive health information laws. Individuals can understand their granular choice related to these categories (e.g., protected by laws in addition to HIPAA, or by provider). These categories and rules should be consistently applied to health information across the United States, no matter where an individual or their health information is.

Table 7: Critical Actions for Consistent Representation of Permission to Disclose Identifiable Health Information

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
G1. Improve Health IT stakeholders' understanding of existing HIPAA rules and how they support Interoperable exchange through permitted access, use and disclosure for TPO	1. Through education and outreach, federal government/Office for Civil Rights (OCR) will consider where additional guidance may be needed to help stakeholders understand how the HIPAA Privacy Rule permits health information to be exchanged (use and disclosure) for TPO without consent. 2. Federal and state governments, in coordination with organizational health information privacy policymakers, conduct outreach and disseminate educational materials and OCR guidance to LHS participants about Permitted Uses and Disclosure of health information and Individual Choice. 3. ONC will brief key stakeholders, possibly including NCSL, NGA, privacy advocates and Congress on findings regarding the complexity of the rules environment, especially the diversity among more restrictive state laws that seek to regulate the same concept, impedes computational privacy. 4. ONC, in collaboration with states, national and local associations, and other federal agencies will convene a Policy Academy on Interoperability with a particular focus on privacy as an enabler of interoperability.	5. Stakeholder input requested	6. Stakeholder input requested

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
G2. Align stakeholder adopted policies with existing HIPAA regulations for health info that is regulated only by HIPAA	For information that is regulated by HIPAA only, ONC will 1. adopt at a policy level a standard definition of what is "Basic Choice" 2. adopt technical standards regarding how to ensure individuals are offered Basic Choice in a manner that can be captured electronically and in a manner in which the individual's choice persists over time and in downstream environments, unless the individual makes a different choice.	3. A majority of state governments and stewards of health information (health care organizations, HIEs, etc.) revise regulations and policies to align with the federal definitions of permitted uses for data regulated solely by HIPAA and also aligning with the ONC standard on what constitutes Basic Choice and how it should be implemented, with the result being an established consensus background rules for the nation.	4. All of state governments and stewards of health information (health care organizations, HIEs, etc.) revise regulations and policies to align with the consensus on non-sensitive information that is permissible to exchange—or access, use and disclose—for TPO without an individual's written consent establishing consensus background rules for the nation.
G3. Align regulations and policies for electronic health info that is protected by laws in addition to HIPAA		1. State governments standardize existing laws pertaining to "sensitive" health information, particularly those regarding clinically sensitive and age-based rules, so that those laws mean the same things in all U.S. jurisdictions, without undermining privacy protections individuals have today. 2. Federal government, a majority of state governments and stewards of health information (health care organizations, HIEs, etc.) begin revising regulations, policies and programs for granular choice to align with the consensus categories of sensitive health information and rules for granular choice that establish consensus background rules for the nation.	3. Federal government, all state governments and stewards of health information (health care organizations, HIEs, etc.) revise regulations, policies and programs for granular choice to align with the consensus categories of sensitive health information and rules for granular choice that establish consensus background rules for the nation.

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
G4. Technical standards for basic choice	1. ONC, standards development organizations, health IT developers and appropriate stakeholders harmonize technical standards and implementation guidance for consistently capturing, communicating and processing basic choice across the ecosystem. 2. Technology developers begin implementing harmonized standards that document and communicate an individual's basic choice.	3. Technology developers implement technical standards and implementation guidance for consistently capturing, communicating and processing individual choice. Adoption has begun, with 5% of exchangers using the standards regularly.	4. Technology developers implement technical standards and implementation guidance for consistently capturing, communicating and processing individual basic choice. Adoption continues, with a majority of exchangers using the standards regularly. 5. Basic choice standards are used widely to electronically capture individuals' desire to have their health information included in research.
G5. Associate individual choice with data provenance	1. ONC, standards development organizations, health IT developers, health care providers and appropriate stakeholders harmonize technical standards and develop implementation guidance for associating individual choice with data provenance to support choice 2. Technology developers begin to implement technical standards for associating individual choice with data provenance to support choice.	3. Technology developers implement harmonized technical standards for associating individuals' choice with data provenance; adoption has begun, with 5% of exchangers using the harmonized standards regularly.	4. Technology developers implement harmonized technical standards for associating individuals' choice with data provenance; adoption has begun, with a majority of exchangers using the harmonized standards regularly.

Consistent Representation of Authorization to Access Health Information

LHS Requirement

H. *Consistent representation of authorization to access health information:* When coupled with identity verification, this allows consistent decisions to be made by systems about access to information.

<table>
<tr><td>FEDERAL HEALTH STRATEGIC PLAN OBJECTIVES SUPPORTED
▸ Protect the privacy and security of health information</td></tr>
</table>

Background and Current State

Authorization represents the scope or amount of information a person or system is allowed to access. After an information recipient/system user has been successfully authenticated, the information holder/system must confirm the user's level of permitted access. This includes both the technical mechanisms and standards for carrying out authorization, whether it is granted based on law, regulation, policy, or an individual's documented choice. Consistent representation of authorization is required for access to an individual's identifiable health information. In a technical environment, when implemented, the information recipient asserts an authorization and the information holder/system evaluates that assertion against national, state or local regulation and, if not inconsistent with applicable law or organizational policies, determines whether to disclose the information.

To be successful, there must be a consistent framework and set of standards so that everyone can agree on when an asserted authorization to receive or access individually identifiable health information is accurate. Therefore, both the requester and the discloser must have a common understanding of what is "authorized," given the requester's role in the individual's care and the purpose of the disclosure.

It is important to note that a disclosure can legally be authorized without a documented choice of the patient, because laws and regulations permit the disclosure without individual consent. An example of this is the HIPAA Privacy Rule's permitted use and disclosure of PHI for TPO by a covered entity. As is discussed in the *Consistent Representation of Permission to Collect, Use and Disclose* functional requirement, individuals may be able to express a choice. This choice, when expressed, should be documented and reflected persistently in the data. Nevertheless, it may not legally be required to obtain an individual's documented choice before exchanging PHI for TPO.

The determination that a disclosure is "authorized" is a legal matter that can be defined by the proposed use of the data (e.g., TPO), the role of the proposed data user (role based access), or the individual's documented choice, or some combination of all three. The role of technical standards is to capture and persistently adjudicate the applicable authorization in the data. Furthermore, if there will be multiple ways of representing and persisting what access, use, or disclosure was authorized, a downstream user needs to respect how someone else has chosen to represent the scope of authorized access, use, or

disclosure, unless there is a definitive, later documented change to the scope of authorized access, use, or disclosure. To date, technical standards to support authorization exist but have not been widely implemented, potentially because of the diverse legal and regulatory environment discussed in the Consistent Representation of Permission to Disclose requirement.

An example of such a technical standard is Security Assertion Markup Language (SAML.) SAML is an XML-based, open standard for exchanging authentication and authorization data between parties consistent with Simple Object Access Protocol (SOAP) web services. The eHealth Exchange has implemented SAML as part of its Authorization Framework. SAML, as used in the Authorization Framework, allows an organization to assert the individual identity, means of authentication, role and purpose for use in a request for disclosure (for query-based transactions or information submission transactions). It includes a standardized enumeration of acceptable authentication methods, roles and purposes. The recipient of a message can use this information to determine whether the request should be honored and disclosure made (whether the authentication type, role and purpose for use are consistent with the policy environment of the discloser) using automated mechanisms.

Moving Forward

A learning health system will need to consider access by providers, public health professionals, consumers and many other authenticated users. These users will possess changing and complex roles with varying authority to use, access or receive health information that will depend on laws, regulations, the user's role and individuals' choices. The specifications for the Authorization Framework must account for the legal, regulatory and individual choice environment, as well as unambiguously identify the types of learning health system data users and the scope of their roles.

As the health IT ecosystem matures to support an evolving nationwide learning health system, both policy and technology will need to support a growing set of intended and authorized purposes for use and provide the information necessary to make clear determinations to disclose electronic health information. A learning health system must also provide sufficient information to log and audit access so that disclosures can be accounted for and audited. Finally, while authorization is not the same as authentication, it critically depends on reliable mechanisms of authentication of individuals and systems involved in information access.

Table 8: Critical Actions for Consistent Representation of Authorization to Access Data or Services

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
H1. Develop New Policies and Regulations	1. ONC will convene workshops or listening sessions on the types of data sharing that may be required, by role, to support value-based purchasing. A major goal of the workshops will be to evaluate how close the nation can come to achieving its goals of the three-part aim using existing privacy rules.	2. Stakeholder input requested	3. Stakeholder input requested
H2. Clarify Existing HIPAA Requirements	1. The HHS Office for Civil Rights will consider where additional guidance may be needed to help stakeholders understand how HIPAA Privacy and Security Rules apply in an environment where ACOs and other multi-stakeholder entities permeate the landscape in support of value-based purchasing.	2. Stakeholder input requested	3. Stakeholder input requested

Certification and Testing to Support Adoption and Optimization of Health IT Products and Services

Certification and testing are approaches used to assess whether health IT meets certain technical requirements, including conformance to technical standards necessary for interoperability. While testing can be performed on its own, certification includes both testing and an additional review by an independent third-party who places its integrity and reputation on the line. Certification is designed to provide confidence to stakeholders without the expertise to individually evaluate whether a product meets specific requirements. Both testing and certification will be needed to support the optimization of health IT products and services.

Stakeholder Assurance that Health IT Is Interoperable

LHS Requirement

I. *Stakeholder assurance that health IT is interoperable:* Stakeholders that purchase and use health IT must have a reasonable assurance that what they are purchasing can interoperate with other systems.

FEDERAL HEALTH IT STRATEGIC PLAN OBJECTIVES SUPPORTED

▸ Increase the adoption and effective use of health IT products, systems and services
▸ Increase user and market confidence in the safety and safe use of health IT products, systems and services
▸ Accelerate the development and commercialization of innovative technologies and solutions
▸ Identify, prioritize and advance technical standards to support secure and interoperable health information

---

Background and Current State

As described in ONC's 10-year vision document, testing and certification are methods that can be used to assure technology users that health IT meets specific technical requirements. Testing and certification can assess standards conformance as well as specific capabilities to support users' interoperability needs across the broad health IT ecosystem.

In 2005, ONC funded the Certification Commission for Health Information Technology (CCHIT) to create the first voluntary health IT certification program. In 2009, the HITECH Act[55] provided the National Coordinator with the authority to establish a program or programs for the voluntary certification of health information technology. To date, the certification criteria adopted by the Secretary have been correlated with and support Meaningful Use objectives and measures specified under the CMS EHR Incentive Programs. During the last several years, many additional conformance testing and certification programs have been developed (often specific to a use case and set of standards, including: Surescripts certification for ePrescribing, IHE Connectathons for IHE profiles, EHNAC and DirectTrust programs for Direct services and many others (see Appendix H for Priority Interoperability Use Cases).

Moving Forward and Milestones

A diverse and complementary set of certification and testing programs will need to be in place to achieve a nationwide learning health system. These certification and testing programs will need to be administered by a variety of different entities both inside and outside of government, but well-coordinated so as not to create conflicting or duplicative requirements for industry stakeholders. Though certification and testing programs exist today, recent focus has been on EHRs or specific capabilities within EHRs. Over time, there will be a need for certification and testing programs for provider and non-provider systems such as network technologies and resources, payer systems, population health resources and systems employed for patient engagement as all of these different technologies become part of a learning health system. Certification in support of a learning health system should be specific and focused on the areas that have the greatest impact on interoperability.

As the market continues to demand interoperability beyond organizational boundaries, certification and testing programs can be a means to more rapidly scale the consistent implementation and use of a common set of technical standards. It is equally important to note that testing in addition to or independent of certification will play a critical role in advancing interoperability. A focus on continuous testing, during health IT development, implementation and post-implementation/use will require broad industry commitment to the development, maintenance and use of testing tools. Testing programs should also incorporate negative testing and exception handling cases to ensure systems are resilient across a broad range of real world interoperability scenarios. Coordinated governance will have a role in reinforcing the use of a common set of standards and testing protocols, which is a foundational step in assuring that health IT can truly be interoperable.

---

[55] Section 3001(c)(5) of the PHSA provides the National Coordinator with the authority to establish a certification program or programs for the voluntary certification of health IT. Specifically, section 3001(c)(5)(A) specifies that the "National Coordinator, in consultation with the Director of the National Institute of Standards and Technology, shall keep or recognize a program or programs for the voluntary certification of health information technology as being in compliance with applicable certification criteria adopted under this subtitle" (i.e., certification criteria adopted by the Secretary under section 3004 of the PHSA).

Table 9: Critical Actions for Stakeholder Assurance that Health IT is Interoperable

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
I1. Testing Tools	1. ONC, NIST and other health IT stakeholders will provide testing tools necessary to support the criteria in ONC's certification program. 2. Health IT developers, SDOs and government will explore and accelerate a suite of testing tools that can be used by implementers post-implementation to ensure continued interoperability while health IT is in use. 3. SDOs begin to develop and maintain additional testing tools in support of more stringent testing of standards.	4. ONC, NIST and other health IT stakeholders will provide updated testing tools in support of ONC's certification program. 5. Health IT Developers, SDOs and government will maintain a suite a testing tools. 6. Health IT developers will regularly use testing tools to maintain interoperability while health IT is in use.	7. ONC, NIST and other health IT stakeholders will provide updated testing tools in support of ONC's certification program. 8. Health IT developers. SDOs and government will maintain a suite of testing tools.
I2. Certification programs	1. Health IT Developers, ACBs, ATLs and other stakeholders will analyze, identify gaps and provide feedback to ONC regarding certification criteria that should be added to the ONC HIT Certification Program. Specifically, criteria that would support ONC's desire to expand the scope of the certification program to support health IT used in a broader set of health care settings, such as criteria for long-term and post-acute care, home and community based services in non-institutional settings and behavioral health settings. Additionally, criteria related to accessibility and usability of health IT. 2. Other existing industry certification programs will continue to complement ONC's certification program to ensure that different aspects of health IT conform to the technical standards necessary for interoperability. 3. FACAs will make recommendations for standards and certification criteria for inclusion in ONC's certification program.	4. Health IT developers, ACBs, ATLs and other stakeholders will continue to provide feedback to ONC regarding certification criteria that could be added to the ONC HIT Certification Program in order to increase its impact on interoperability 5. ONC and other industry certification programs will focus on including more stringent testing such as scenario-based testing and post-implementation testing to ensure interoperability while health IT is in use.	6. ONC and other industry certification programs will continue to update criteria as needed in support of a learning health system's evolving needs, new standards and expanded program's scope to include health IT used in a broader set of health care settings

Core Technical Standards and Functions

Core technical standards must be widely deployed and advanced to enable nationwide interoperability. The consistent implementation and use of standards as well as broad access to technology services is foundational for a learning health system to mature over the next 10 years. The ability for health professionals to collect health information in structured formats, share such information in a seamless manner and for that information to be usable at the time it is needed as well as be re-useable for additional permitted purposes will be key to advancing a learning health system.

Standards often seek to accommodate the complexity inherent in medicine and the business of health care. In general, standards are developed in response to a specific clinical and/or business need (often referred to as a "use case"). Standards are also specified at different levels and combined in different ways in order to properly address a use case and its expected data requirements (see Appendix H for Priority Interoperability Use Cases). Typically five types of standards (and accompanying implementation specifications) are necessary and used together in order to achieve interoperability for a given purpose (see Figure 8):

1. **Vocabulary/terminology standards** that are unique to health care and often purpose-specific (e.g., codes to represent medications cannot be also used for lab tests);
2. **Content/structure standards** that are also usually unique to health care, are often purpose-specific and often designed to represent data captured from a specific clinical workflow (e.g., the content standard used for electronic prescribing would not be used for a referral to a specialist).
3. **Transport standards** that are typically non-unique to health care because they are used to connect two or more parties together without a focus on the data that would be transported from one party to another.
4. **Security standards** that are non-unique to health care and often applied in different ways to meet the data protection requirements specified by a use case (although in health care there are legal minimums for functional security outcomes stated in the HIPAA Security Rule.) In any event a security standard supports achieving the security outcomes prescribed by the Security Rule. These standards are discussed in the privacy and security protections building block.
5. **Standards for Services** that typically represent technical infrastructure used to simply connect different systems together to perform actions in order to support the accomplishment of a use case. These are discussed further in the Secure, Standards Services section and include, but are not limited to APIs that enable systems to talk to each other.

Figure 8: Standards Categories

CATEGORIES OF STANDARDS	FUNCTIONS OF STANDARDS	EXAMPLES OF REAL WORLD USE OF THE STANDARDS
VOCABULARY & CODE SETS (SEMANTICS)	The information is universally understood	RxNorm Code for Ibuprofen is 5640
FORMAT, CONTENT & STRUCTURE (SYNTAX)	Information is in the appropriate format	C-CDA packages up data in the appropriate format
TRANSPORT	The information moves from point A to point B	SMTP and S/MIME to send the C-CDA from one setting to another
SECURITY	The information is securely accessed and moved	X.509: to ensure it is securely transmitted to the intended recipient
SERVICES	Provides additional functionality so that information exchange can occur	DNS+LDAP: to find the recipient's X.509 certificate to encrypt a message

Consistent Data Formats and Semantics

LHS Requirement

J. *Consistent Data Formats and Semantics:* Common formats (as few as necessary to meet the needs of learning health system participants) are the bedrock of successful interoperability. Systems that send and receive information generate these common formats themselves or with the assistance of interface engines or intermediaries (e.g., HIOs, clearinghouses, third-party services.) The meaning of information must be maintained and consistently understood as it travels from participant to participant. Systems that send and receive information may or may not store standard values natively and therefore may rely on translation services provided at various points along the way.

FEDERAL HEALTH IT STRATEGIC PLAN OBJECTIVES SUPPORTED

▸ Identify, prioritize and advance technical standards to support secure and interoperable health information
▸ Increase access to and usability of high-quality electronic health information and services
▸ Invest, disseminate and translate research on how health IT can improve health and care delivery

---

Background and Current State

In the same way goods are packaged before being shipped so that they arrive at their destination safely, standardized data formats are the way electronic health information is packaged or structured so that one system can use the information that is sent by another system. When a computer system receives electronic health information from another system, it needs to process the information automatically, without time-consuming human intervention. This can only occur if the sending system has used a consistent data format that is known to – and expected by – the receiving system. Given the number of different systems that must exchange health data, it would be virtually impossible and grossly inefficient for each system to negotiate agreed-upon exchange formats with all other systems with which it interacts. The most practical solution is for all systems to follow the same standards for specific health data exchanges so that sending and receiving systems and users of those systems will be able to receive, interpret correctly, integrate and use data generated by other systems.

If sending and receiving systems are not developed and configured to adhere to a common and consistent set of standards for a particular use, then the users of those systems will have difficulty with interoperability. For example, while a health professional would readily understand that "Tylenol" and "acetaminophen" are used synonymously; two computer systems exchanging those phrases may treat the terms entirely different, if not bound to a standardized vocabulary or terminology.

Semantics are the vocabularies and coding systems used to represent clinical information in a health IT system. Semantic interoperability is the "ability to automatically interpret the information exchanged meaningfully and accurately in order to produce useful results as defined by the end users of both systems."[56] Several vocabulary and terminology standards are already adopted by ONC in regulation and are required in the 2014 CEHRT definition and subsequently meaningful use stage 2[57]. This includes, but is not limited to: Systematized Nomenclature of Medicine-Clinical Terms (SNOMED CT) for problems or conditions, RxNorm for medications and medication allergies, or Logical Observation Identifiers Names and Codes (LOINC) for laboratory tests and CVX for immunizations. Additionally, other vocabulary and terminology standards are embedded within the implementation guides documenting the use of data formats such as HL7 v2 messages and C-CDA. In many cases, "value sets", such as those published in the Value Set Authority Center (VSAC), are established to identify subsets of the standard vocabularies to be used for a specific purpose. For example, for the purposes of quality measurement, all the relevant codes from SNOMED-CT and/or LOINC that can be used to identify diabetic patients for quality measurements in EHRs are put in a specific list.

Several format standards are already adopted by ONC in regulation and required for the purposes of 2014 Edition certification and subsequently meaningful use. This includes, but is not limited to: Consolidated Clinical Document Architecture (C-CDA), HL7 v2 and NCPDP SCRIPT. There are various

---

[56] CEN/ISO 13606. http://www.en13606.org/the-ceniso-en13606-standard/semantic-interoperability

[57] http://healthit.gov/policy-researchers-implementers/certification-and-ehr-incentives

information models and representations of data that are used and directly referenced by these semantic and format standards. These models provide an agreed upon representation of data that engineers and developers can understand, use and ultimately implement. Information models are necessary to provide commonality and consistency in the representation of the data and drive data to a semantic level that provides consistent meaning across multiple systems. The complexity of having the various formats, vocabularies, terminologies and information models makes interoperability of health IT much more challenging than other industries, such as ATMs, credit card processing and airline reservation systems.

Standards Development Organizations (SDOs) are primarily responsible for developing, curating and maintaining all of the standards mentioned above as well as any accompanying information models. These organizations include, but are not limited to: Health Level 7 (HL7), the National Council for Prescription Drug Plans (NCPDP), Integrating the Healthcare Enterprise (IHE), Clinical Data Interchange Standards Consortium (CDISC), Regenstrief Institute, IHTSDO, National Library of Medicine (NLM) and the National Center for Health Statistics under CDC. In addition to publishing standards, these organizations also create profiles or implementation specifications/guides that provide additional implementation instruction to developers based on the particular purpose for which the standard is intended to be used. For instance, the HL7 2.5.1 standard is a content standard for which several different implementation guides have been created to address specific purposes ranging from lab result receipt to immunization submission.

In some cases the implementation guides provide sufficient clarity, specific implementation instructions and reduce the potential for implementation variability to a minimum. In other cases, further work is necessary among SDOs to further refine implementation guidance as well as to develop best practices to improve implementation consistency among health IT developers.

Consistent Format: Consolidated Clinical Document Architecture (C-CDA)

Though much of the industry has implemented C-CDA as it is required in 2014 CEHRT and subsequently Meaningful Use stage 2, there is significant variability in the implementation of the standard. Often, international health IT standards are designed to satisfy many different requirements and leave the developer with significant choices on how to implement pieces of the standard. While some portions of the C-CDA implementation guide are required and have a required vocabulary/terminology, other segments of the C-CDA are optional or required but do not designate specific vocabularies. This variability in implementations does not allow a receiving

> **A Common Clinical Data Set**
>
> ‣ Patient name
> ‣ Sex
> ‣ Date of birth
> ‣ Race
> ‣ Ethnicity
> ‣ Preferred language
> ‣ Smoking status
> ‣ Problems
> ‣ Medications
> ‣ Medication allergies
> ‣ Laboratory test(s)
> ‣ Laboratory value(s)/result(s)
> ‣ Vital signs
> ‣ Care plan field(s), including goals and instructions
> ‣ Procedures
> ‣ Care team members
> ‣ Immunizations
> ‣ Unique device identifier(s) for a patient's implantable device(s)
> ‣ Notes/narrative

system to process the information and properly integrate it into the patient record and may even prohibit the end user from viewing the information in a human readable format. Consequently, providers and hospitals are sending summary of care records at an extraordinary rate, but the receiving providers' systems often cannot display the summary of care, let alone incorporate its contents into the patient's record. Therefore, more guidance on how to consistently implement the standard is needed in order to support interoperability. Some say further constraint to this international standard is necessary to support interoperability.

In order to support exchange across the continuum of care and in support of a learning health system, interoperable data formats must be adopted for care settings such as behavioral health, long-term and post-acute care (LTPAC) and community service providers (e.g., schools, prisons and social services) and also by the research community. The S&I Framework[58] Longitudinal Care Coordination initiative, launched in 2012, worked on modifying the C-CDA to include things like care plans that would support, in particular, LTPAC communities. The initiative completed its work in September 2014 with the C-CDA R2 updates. A new S&I Framework initiative, electronic Long-Term Services and Support (eLTSS), has been working to build consensus use cases to support care settings such as behavioral health and community service providers and ultimately create a data format that incorporates needed data elements in a standardized fashion to support the use cases. The eLTSS initiative was recently launched and therefore has not completed significant work to date.

Moving Forward and Critical Actions

Over time (and for a learning health system to rapidly innovate), it will be necessary for the industry to converge and agree on the use of the same content and vocabulary standards to satisfy each specific interoperability purpose. The use of multiple data formats over the long term is not sustainable and retains systemic costs and burdens that could otherwise be removed from the health care system for health IT developers, providers and individuals. Content standards should continue to accommodate the exchange of structured and unstructured data, but developers and end-users should design and subsequently implement systems with a very intentional movement and bias toward increased exchange of more structured, standardized and discrete information.

At a minimum, we must as a nation agree to a standardized common clinical data set[59] that is consistently and reliably shared during transitions of care (and with individuals and their caregivers) to achieve our near-term goal of establishing a foundation of interoperability that can be expanded over time. The industry seeks significant progress in the standards that support structured information so that the information can be computable and usable by other systems and ultimately users of those receiving systems. However, stakeholders have also made it clear that there remains value in the

---

[58] http://wiki.siframework.org/

[59] Vitals, in particular, should be expanded to include – patient's body height, body weight measured, diastolic and systolic blood pressure, heart rate, respiratory rate, body temperature, oxygen saturation in arterial blood by pulse oximetry, body mass index (ratio). Vitals should also include date and time of vital sign measurement or end time of vital sign measurement and the measuring- or authoring-type source of the vital sign measurement

documentation and exchange of some unstructured data, such as a physician note that is typically documented as free text in a system.

While it is unlikely that a single data format (at least structured as a document) will support all of the needs of a learning health system, every effort should be made to minimize not only the number of data formats, but also to have agreement on the use cases that each data format supports (see Appendix H for Priority Interoperability Use Cases). This will be even more challenging when social services, genomic, personally generated information, environmental sciences and other forms of information have to be integrated to support a learning health system. Initiatives such as the National Information Exchange Model (NIEM)[60] may be helpful when needing to exchange across sectors (see Appendix E for more on NIEM).

Over the long-term, document-centric ways of exchanging electronic health information will likely be overtaken by more specific, tailored, data-centric ways of exchanging information – meaning that individual data elements are exchanged (e.g., medications or allergies) rather than an entire document with multiple information sections about a patient. This will allow electronic health information to be defined (and reused) in a more granular fashion and create more flexibility in how information is used. To do this, over the next six to ten years, the industry will need to develop standards for granular data elements that can be used in documents and move toward ways of exchanging information that do not require information to be in document form. HL7's Fast Healthcare Interoperability Resources (FHIR)[61] effort is one effort that is emerging and exploring ways to accommodate new methods of exchanging information. Importantly, it will be increasingly necessary for the industry as a whole to invest time in thoughtfully planning the migration and transition from one standard to another as well as from one version of a standard to a newer version.
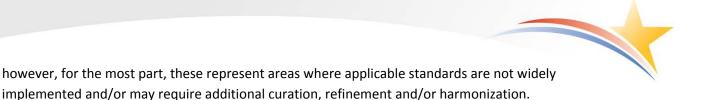
To support clinical care, research, quality measurement and clinical decision support, a learning health system may need, for some environments and purposes, to shift from static code lists that define a concept within a single application or organization to more systematic, shared ways of representing meaning. This will allow computers to automatically update and reason about meaning or connect different codes together to create more complex concepts. This would require NLM and other industry leaders to help guide the processes by which this automation can occur. Furthermore, the industry should embrace the idea of making service calls to access the most up-to-date vocabularies rather than trying to manage these vocabularies locally in their systems.

The list below is a non-exhaustive set of standards activities that are being worked on actively by various standards communities and SDOs **(and for which others should recommend additions during the Roadmap's comment period.)** SDOs such as HL7 and IHE are collaborating in many ways with these particular standards efforts. In some cases, there are pockets of implementation and pilot activities,

---

[60] https://www.niem.gov

[61] http://www.hl7.org/implement/standards/fhir/summary.html

however, for the most part, these represent areas where applicable standards are not widely implemented and/or may require additional curation, refinement and/or harmonization.

- HL7 Fast Healthcare Interoperability Resources (FHIR™)[62] Work Group including, but not limited to, standards in support of RESTful APIs
- Clinical Information Modeling Initiative (CIMI)[63] including, but not limited to, supporting an open repository of standardized, detailed clinical information models
- NCPDP-HL7 Pharmacist/Pharmacy Provider Functional Profile Task Group[64]
- NCPDP MC Real-Time Prescription Benefit Inquiry Task Group[65]
- ONC S&I initiative[66] - Data Access Framework (DAF) including, but not limited to, standards that support a targeted query for granular data and documents
- ONC S&I initiative - Quality Improvement (QI) including, but not limited to, a harmonized data model for quality measurement and clinical decision support (CDS)
- ONC S&I initiative - Structured Data Capture (SDC) including, but not limited to, a standard for the structure of Common Data Elements (CDEs)
- ONC S&I initiative - Prescription Drug Monitoring Program (PDMP) including, but not limited to, an IG that references several standards
- ONC S&I initiative - Electronic Long Term Support Services
- ONC S&I initiative - Data Provenance
- ONC S&I initiative - Data Segmentation for Privacy
- NIEM[67] Human Services and Health emerging domains

---

[62] http://www.hl7.org/implement/standards/fhir/summary.html

[63] http://opencimi.org/

[64] http://ncpdp.org/Standards/Work-Group-Listing

[65] http://ncpdp.org/Standards/Work-Group-Listing

[66] http://wiki.siframework.org/

[67] http://www.niem.gov

Table 10: Critical Actions for Consistent Data Formats and Semantics

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
J1. Common, list of interoperability standards	1. ONC will annually publish and update a list of the best available standards and implementation guides supporting interoperability in order to enable priority functions in a learning health system, to be used by technology developers and to inform coordinated governance efforts. ONC will create this list through an open and transparent process that facilitates competition between standards for selection. To the extent possible, the updates to this list will be done in a manner to minimize unnecessary sunk costs and to promote the entry of innovative standards. 2. Technology vendors, certification programs and governing bodies should use ONC's list of the best available standards when making decisions about the standards they will use to enable specific use cases. 3. Provider and patient-facing technology developers will update their systems to align with the list of the best available standards, in particular, C-CDA 2.0 and associated vocabulary standards and code sets that support a common clinical data set.	4. ONC will annually publish an updated list of the best available standards and implementation specifications.	5. ONC will annually publish an updated list of the best available standards and implementation specifications.
J2. Architecture in support of standards activities	1. Through coordinated governance, public and private stakeholders will establish and maintain a prioritized set of use cases and associated functional requirements for delivery system reform and a learning health system (see Appendix H for Priority Interoperability Use Cases). 2. Through coordinated governance, public and private stakeholders will develop a nationwide technical architecture for an interoperable learning health system. 3. Through coordinated governance, public and private stakeholders will define a necessary set standards activities that support the prioritized use cases and functional requirements and the agreed upon architecture.	4. Stakeholder input requested	5. Stakeholder input requested

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
J3. Develop and pilot new standards for priorities	1. SDOs will advance and accelerate semantic standards for lab orders, other orders and other priorities for a LHS that require updated or new semantic standards 2. Research and clinical trial communities will pilot the use of the common clinical data set. 3. SDOs will advance consumer-friendly terminologies. 4. Health IT developers and SDOs should advance systems in support of human-centered design for systems, including the ability to provide information to individuals with varying levels of health literacy so individuals can understand their electronic health information and ability to provide information in their primary language. 5. Technology developers, providers and individuals will pilot data format and vocabulary standards in order to provide feedback to the SDOs for further refinement. 6. States and other stakeholders across the ecosystem to further explore and determine the role that NIEM can serve with regards to supporting health care and human services interoperability. 7. SDOs and industry will collaborate and agree on best practices and provide guidance on the exchange of unstructured data such as a physician note.	8. Stakeholder input requested	9. Stakeholder input requested
J4. Vocabulary approach	1. Through coordinated governance, public and private stakeholders will work with SDOs to define a standard approach to federated distribution of centrally maintained code sets. 2. Health IT developers will provide accurate translation and adapter services where needed in order to support priority learning health system use cases (see Appendix H for Priority Interoperability Use Cases).	3. Stakeholder input requested	4. Stakeholder input requested
J5. Maintain and improve standards	1. SDOs will maintain and improve existing standards based on implementation feedback.	2. SDOs will maintain and improve standards.	3. SDOs will maintain and improve standards.
J6. New standards that support new and evolving requirements and priorities	1. Through coordinated governance, public and private stakeholders will advance the development and maintenance of data format and vocabulary standards and implementation guidance necessary to support priority learning health system use cases (see Appendix.)	2. Stakeholder input requested	3. Stakeholder input requested

Secure, Standard Services

LHS Requirement

K. *Standard, secure services:* Services should be modular, secure and standards-based wherever possible.

FEDERAL HEALTH IT STRATEGIC PLAN OBJECTIVES SUPPORTED

▸ Increase access to and usability of high-quality electronic health information and services
▸ Identify, prioritize and advance technical standards to support secure and interoperable health information

---

Background and Current State

Secure, standard services support functional capabilities, including Direct secure messaging, query and publish/subscribe. In particular, the S&I Framework's Data Access Framework initiative (DAF) is evolving existing IHE standards in support of query services. The adoption of a service-oriented architecture (SOA) is fundamental to using standard services for interoperability. The concept of SOA is not new; for years, software developers have created systems with application programming interfaces (APIs) that define how systems and subsystems interact with one another by exchanging data in reliable, structured ways.

All of the core services that are used to operate the Internet began as functions with APIs. Many of these core services and APIs eventually developed into internationally recognized, open standards. In an SOA, complex systems are made available to other systems on a network and perform specific tasks. These services form system building blocks, capable of being reused over and over again in the context of different needs and applications. Diverse systems can share algorithms, features and capabilities by relying on these shared services rather than reproducing this functionality each time it is needed. Users do not need to know or be concerned about the existence of an SOA within the systems they are using. Using an SOA can dramatically reduce the cost and complexity of building and adapting systems to changing needs and environments.

One of the guiding principles for the Roadmap is the notion of *modularity*: complex systems are more durable under changing circumstances when they are divided into independent components that can be connected together. SOA is at the core of the modularity required by a learning health system. But in order for interoperability to function on a wide scale, the APIs (which represent the points of contact, or boundaries, between disparate systems) need to be consistent and standardized as much as possible. Such "loose coupling" means that not all systems within organizations need to perform the same functions identically (or at all), only that when they choose to request access to data or services from each other. What's more, they should do so in predictable ways agreed upon by learning health system participants.

While many systems are proprietary in nature, some health IT developers publish their API specifications to enable other systems to interoperate with them. This publication of APIs reduces complexity by focusing standardization solely on those well-defined functions and data elements that need to be used in interoperable health IT systems. At the scale at which a learning health system will operate, however, simply publishing APIs is not enough; there must also be a limited number of standard APIs to reduce complexity.[68]

In some industries, simply publishing APIs has led to enough market standardization to enable interoperability. In other industries, more assertive top-down coordination has been needed. To date, health IT technology developers have not prioritized making APIs available that could be broadly and easily used to achieve core interoperability use cases and fuel innovative, market-led interoperability.

While every effort should be made to use as few strategies as possible to achieve health IT interoperability, a second guiding principle is that there is no "one-size-fits-all solution." This tension requires careful coordination among participants and the willingness to adopt solutions that may not currently be in use within a particular organization or segment of the industry.

Moving Forward and Milestones

The services envisioned in this Roadmap are consistent with the vision of the JASON Report, *A Robust Health Data Infrastructure*, released in April 2014. The Roadmap also considers the recommendations of the HIT Policy Committee JASON Task Force.

While it may take several years to achieve, a learning health system must converge on a limited set of APIs to support the services that are needed. However, there is a delicate tension that emerges: new features continue to be conceptualized, new work flows are created and new APIs and standards are developed; at the same time, existing functionality cannot be easily or quickly abandoned or replaced. While the Roadmap will identify a limited set of APIs and standards that are needed to support a learning health system in the short term, coordinated governance will continue to identify, select and help transition the industry to new APIs and standards whose functionality has been replaced or eclipsed.

---

[68] The April 2014 JASON Report, A Robust Health Data Structure, recommended that, "interoperability issues can be resolved only by establishing a comprehensive, transparent and overarching software architecture for health information." The report further defines architecture as "the collective components of a software system that interact in specified ways and across specified interfaces to ensure specified functionality." In this context, the report goes on to call for standards, interfaces and protocols that are open and APIs that are public. Following the JASON Report, the HIT Policy Committee convened a task force to review the report's recommendations and subsequently advise ONC on the adoption of the report's recommendations. The task force called for a coordinated architecture that, rather than being top-down in nature, would be more loosely coupled, enabled by public APIs defined by the group as uniformly available, non-proprietary, tested by a trusted third party and operating within well-define business and legal frameworks. See the Introduction section of the Roadmap for links to these reports.

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
K1. APIs	1. Through the coordinated governance process, health IT developers, SDOs, ONC and others should implement a coordinated approach to developing and standardizing a targeted set of public APIs for nationwide interoperability. 2. Health IT developers should work with SDOs to develop public APIs for sending, receiving and finding a common clinical data set. 3. ONC and other certification bodies should develop approaches through certification that encourage the adoption of specific APIs or consistently functioning APIs in a manner that, while reducing switching costs, does not prevent the adoption of innovative new APIs. 4. SDOs should advance and accelerate the development of standardized RESTful APIs. 5. Health IT developers should work with SDOs to develop standards for interoperable electronic health devices.	6. Stakeholder input requested	7. Stakeholder input requested

Consistent, Secure Transport Techniques

LHS Requirement

L. *Consistent, secure transport technique(s):* Interoperability requires transport techniques that are vendor-neutral, easy to configure and widely and consistently used. The fewest number of protocols necessary to fulfill the needs of learning health system participants is most desirable.

FEDERAL HEALTH IT STRATEGIC PLAN OBJECTIVES SUPPORTED

▸ Identify, prioritize and advance technical standards to support secure and interoperable health information
▸ Increase access to and usability of high-quality electronic health information and services

---

Background and Current State

Transport techniques are the means by which data gets from one place to another. Transport techniques are data agnostic, meaning the content of what is being sent should be irrelevant to the operation of the transport protocol. Interoperability requires transport techniques that are vendor-neutral, easy to configure and widely adopted. It is also desirable for the fewest number of protocols necessary be used to fulfill participants' needs. Security techniques such as the encryption of data in transit and assurance that data only goes to the intended recipient (individual or system) are of prime concern (these issues are discussed elsewhere in the Roadmap).

There are currently several transport techniques widely adopted today. Due to ONC's 2014 edition certification requirements, requirements in the CMS EHR Incentive Programs and ONC's State HIE Program, the Direct transport protocol (commonly called Direct) has seen increasing adoption within the industry. Direct was created to lower the barriers to exchange by creating a protocol that used existing email transport protocols in a secure way. While the implementation of Direct is fairly straightforward technically, it also requires trust to be established by the trading partners involved, which has posed challenges to its widespread use.

Another major transport technique uses web services. Simple Object Access Protocol (SOAP)-based web services often leverage IHE profiles and support transport for queries, as well as services like public health reporting. The eHealth Exchange also uses SOAP-based web services in its implementation. This strategy is becoming more popular among EHR vendors as it allows XML-based, system-to-system transactions to be constructed easily. Another type of web service approach includes RESTful implementations, which are being leveraged by the S&I Framework's RESTful Health Exchange (RHEx) project and HL7's Fast Healthcare Interoperability Resources (FHIR) project.

Moving Forward and Milestones

A suite of transport standards will continue to be developed and maintained to support various interoperability needs, in particular those priorities identified through a coordinated governance process based on the architecture of a learning health system. The suite of transport standards should be consistent with core Internet technologies that are pervasively deployed. Direct is one such core technology for sending information between known parties. Web services based on SOAP and RESTful approaches will continue to be used for more automated transactions, including query/response and some "push" transactions. Additionally, secure transport techniques will be necessary to support individual sharing of personal health information, as well as patient-generated data.

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
L1. Common Transport Standards	1. ONC will identify, and health IT developers should adopt, a minimum set of common transport standards to enable priority learning health system functions. 2. SDOs should update standards and health IT developers should adopt standards as needed.	3. SDOs should update standards and health IT developers should adopt standards as needed.	
L2. Send	1. Public health agencies should converge on the use of standardized web services to support data submission as well as data query from registries and other systems. 2. Providers (including hospitals, ambulatory providers, long-term care centers and behavioral health providers) should adopt and use DIRECT to reach critical mass. 3. Providers and health IT developers should provide individuals with the ability to easily and securely transport their health data to a destination of their choice.	4. Stakeholder input requested	5. Stakeholder input requested
L3. Receive and Find	1. Health IT developers, providers and researchers should increase use of national standards for query functionality 2. Health IT developers, providers and public health agencies should increase use of national standards for publish/subscribe functionality. 3. SDOs should pilot, assess and refine standards for RESTful web services. 4. Health IT developers should widely implement national standards for query. 5. Health IT developers should widely implement national standards for publish/subscribe. 6. Health IT developers should implement national standards for RESTful web services as they are available.	7. Stakeholder input requested	8. Stakeholder input requested

Accurate Individual Data Matching

LHS Requirement

M. *Accurate identity matching:* Whether aggregated in a repository or linked "just in time," health information from disparate sources must be accurately matched to prevent information fragmentation and erroneous consolidation. As a learning health system evolves, more than individual/patient-specific information from health records will be matched and linked, including provider identities, system identities, device identities and others to support public health and clinical research.

▸ Identify, prioritize and advance technical standards to support secure and interoperable health information
▸ Increase access to and usability of high-quality electronic health information and services

Background and Current State

Individuals' health information is often stored in multiple systems, even within a single health organization. Inaccurate identity matching poses a significant patient safety risk, reduces health care efficiency and creates concerns regarding data integrity and compliance with any restrictions on the use of their health information that an individual has made in executing his/her authorizations. There is a significant near-term need to focus on identity matching for clinical care, so that patients can receive safe and effective care at every point of care. However, there is a long-term need to consistently and accurately match individual data for public health purposes to support investigation and to also support research and administrative claims processing and payment.

Identity matching should not be confused with authentication. Authentication is used to verify that the person seeking access to data is the same person that they claim to be (i.e., , prevent someone from using someone else's identity to access a system.)

Identity matching for clinical care has primarily relied on the use of data points that identify patients as uniquely as possible, such as name, address, etc. (known as patient demographics) and sophisticated matching processes. Patient identity matching also uses technologies such as master or community patient indexes and deterministic and probabilistic matching algorithms.[69] Since matching is usually reliant on patient demographic data, this data's quality has a significant impact on the accuracy of the match. At least one study found that the majority of identification errors in emergency departments could be traced back to patient demographic data being incorrectly entered during the registration process.[70] Ultimately, poor data quality in one system leads to inaccurate identity matching in another.

When requesting patient records from electronic health record systems, there are at least two technical profiles for identity matching in common use today. Both profiles were created and are maintained by IHE[71]: Patient Identifier Cross Referencing (PIX)/Patient Demographics Query (PDQ), for internal system use and Cross-Community Patient Discovery (XCPD) for external use. These profiles describe the method

---

[69] While HIPAA required the creation of national identifiers for patients, providers, hospitals and payers in 1996, subsequent legislation prohibited HHS from funding the promulgation or adoption of a national unique patient identifier. Public Law 105–277. 105th Congress. October 21, 1998. http://www.gpo.gov/fdsys/pkg/PLAW-105publ277/pdf/PLAW-105publ277.pdf

[70] The nature and occurrence of registration errors in the emergency department. AF Hakimzada, RA Green, OR Sayan et al. Int J Med Inform. 2008; 77:169-175. http://www.ncbi.nlm.nih.gov/pubmed/17560165

[71] These IHE profiles are available at http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf and http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf

used to send patient data element queries within an organization (PIX/PDQ), or externally to another organization (XCPD) to ask if it has records matching a specific patient and for that receiving organization to respond whether or not it has records.

The second major component to matching is the matching method itself. There are two primary methods in use today: deterministic matching and probabilistic matching (i.e., , algorithm and tuning). Deterministic matching uses sets of pre-determined rules to guide the matching process and normally requires that data elements match exactly. Probabilistic matching is a process where an estimate is made of the probability that two records are for the same person based on the degree to which certain fields in the two records match. Two thresholds are then set: all record pairs whose probability is above the higher threshold are considered to be matches. All record pairs whose probability is below the lower threshold are not considered matches. The disposition of record pairs whose probability falls in between the two thresholds is considered to be uncertain and they require additional review, likely by a trained staff member.[72] Both of these matching methods, as well as a combination of the two, are used across the industry and there has not been a significant study on which method performs better.

In 2013, ONC undertook an environmental scan on identity matching across the country. The scan included health systems, EHR vendors, health information exchange vendors and master patient index vendors. The environmental scan found that data quality was identified by nearly all participants as a key issue in identity matching. Additionally, few organizations had insight into how well they are performing on identity matching, with very few able to report false positive and false negative rates and in fact, disagreement amongst the organizations on what should be being measured in matching. Finally, there was not unilateral agreement in the industry on which match methods work the best.

Moving Forward and Critical Actions

There is a significant near-term need to focus on patient identity matching in order for other learning health system processes to be able to be fully supported in the next ten years. Consequently, the three-year milestones focus primarily on improving patient matching processes, standardizing data elements and developing best practices for improving data quality. Additionally, there is a significant need to measure the accuracy of patient identity matching processes, so that systems can identify where improvements must be made. Since universal performance metrics do not currently exist and there is little agreement in the industry on what should be measured near-term milestones focus on gaining agreement in the industry on performance metrics. As we move towards a learning health system, the milestones reflect a shift towards identity matching of all participants.

The 2014 patient matching report identified an initial list of data elements that should be included in exchange transactions in a standardized, consistently formatted manner. The list was based on recommendations in 2011 from the HIT Standards Committee and expanded based on feedback

---

[72] Record linkage software in the public domain: A comparison of Link Plus, the Link King and a "basic" deterministic algorithm. Campbell, K. M., Deck, D., & Krupski, A. Health Informatics Journal, 14(1), 5–15: 2008. http://jhi.sagepub.com/content/14/1/5.long

gathered during the environmental scan. The data elements listed below are a starting point for standardization:

- First/Given Name
- Current Last/Family Name
- Previous Last/Family Name
- Middle/Second Given Name (includes middle initial)
- Suffix
- Date of Birth
- Current Address (street address, city, state, ZIP code)
- Historical Address (street address, city, state, ZIP code)
- Current Phone Number (if more than one is present in the patient record, all should be sent)
- Historical Phone Number
- Gender

Data quality must also be addressed. Accurate data collection during the registration process is the first and potentially most important contributor to matching data later. However, few if any industry best practices exist for registrars and front desk staff to accurately record data or for patients to update their data via a portal or online record. While some organizations have established training programs for registrars, many have not. There is a significant need for the industry and front desk staff to establish and document best practices for ensuring data quality at the point of registration. In 2013, ONC released the SAFER guide[73] that included best practices for recording patient demographic data. The industry can build upon these best practices as a starting point.

There is little agreement in the industry on what should be measured inpatient matching (i.e., false positives, false negatives, successful matches, specificity, etc.) Performance metrics need to be universally defined with the expectation that performance thresholds can be established based on the care setting. This would remove the 100% perfect-match barrier. Also, by defining the performance metrics, an industry accepted level of accuracy can be established. The performance metrics need to consider not only the algorithm but also processes and data quality. This should ultimately lead to the development of Acceptable Risk Models for various use cases that require identity matching (e.g., all payer claims databases, PDMP, clinical care).

Not only do the performance metrics need to be agreed on, but tools also need to be developed that allow for measurement by health systems and ambulatory practices. To develop these testing tools, sources of gold standard data (manually viewed linked records, reviewed by at least two reviewers) will need to be established. Or a process will need to be established in which individual institutions can sample and empirically measure their match rates using commonly used information retrieval performance metrics. Additionally, there will need to be a list of patient match scenarios that different

---

[73] http://www.healthit.gov/safer/guide/sg006

organizations can compare against, (i.e., matching for public health and Accountable Care Organizations (ACOs)) as they will have different performance metrics than for matching a clinical record for care.

Finally, while hospitals and ambulatory providers use systems that match patient records, other stakeholders in the care continuum do not necessarily have systems capable of matching individual data with a high accuracy level. There is a need in the near-term for these stakeholders to adopt matching technology. Additionally, as performance metrics and acceptable risk models are developed and tested, organizations will need to use the metrics to help with refining them and to ensure the nation is making progress towards more accurate individual data matching.

Table 13: Critical Actions for Accurate Individual Data Matching

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
M1. Standards and Best Practices	1. ONC and SDOs should standardize the minimum recommended data elements to be consistently included in all queries for patient clinical health information, and to be used to link patient clinical health information from disparate systems. 2. Through coordinated governance, public and private stakeholders should work with standards development organizations to require a set of data elements in all individual identity query and record linking transactions. 3. Through coordinated governance, public and private stakeholders should establish and document best practices for the following processes: patient registration, patient verification of information and patient updates and corrections to information. 4. Through coordinated governance, public and private stakeholders should designate the API capabilities necessary to support individual identity search and individual identity linking transactions.	5. Health IT developers should reliably include standardized identity matching data elements in exchange transactions. 6. Through coordinated governance, public and private stakeholders should ensure that identity matching services use standardized attributes in standardized data formats to match individuals to their data for care coordination, individual use and access. 7. Through coordinated governance, public and private stakeholders should identify, test and adopt additional identity matching data elements, including voluntary data elements. 8. As evidence suggests, ONC and SDOs should standardize additional, required elements for identity matching.	9. Providers and health IT developers should use best practices for data quality and algorithms to enhance identity matching accuracy in a majority of identity matching services.

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
M2. Pilots and Further Study	1. Through coordinated governance, public and private stakeholders should develop and pilot tools and technologies for establishing performance metrics for individual identity, query and internal individual matching/record linking. 2. ONC will coordinate with industry stakeholders and other HHS initiatives to test scenarios that represent a variety of matching settings with the purpose of providing further direction for scalable solutions, standards and best practices. 3. ONC will coordinate with industry stakeholders to study voluntary collection of additional identity attributes, which may include biometric technologies, cell phone number, email address, etc.	4. Stakeholder input requested	5. Stakeholder input requested
M3. Adoption	1. ONC among other stakeholders should begin coordination and dissemination of best practices on identity matching.	2. A broad range of health care settings, including long term care, infusion centers and mental health facilities should consistently use identity matching technologies and processes.	3. All health IT systems should continue to exchange data that includes standardized identity matching data elements 4. Through coordinated governance, public and private stakeholders should ensure that data quality rates within source systems and identity matching services are within acceptable levels as defined by agreed upon performance metrics.

Reliable Resource Location

LHS Requirement

N. ***Reliable resource location****: The ability to rapidly locate resources, including provider, individuals, APIs, networks, etc. by their current or historical names and descriptions will be necessary for a learning health system to operate efficiently.*

FEDERAL HEALTH IT STRATEGIC PLAN OBJECTIVES SUPPORTED

▸ Identify, prioritize and advance technical standards to support secure and interoperable health information
▸ Increase access to and usability of high-quality electronic health information and services

---

Background and Current State

Resource location is the electronic means for discovering participants of a learning health system and the services they provide for sharing or accessing data. A learning health system will include a complex and expanding ecosystem of participants and services, using an evolving set of standards. It will require a means to electronically and conveniently locate participants of interest and services that provide the needed data resources. Resource location services must support a wide range of exchange and data access types, from searching for an individual provider's Direct address so a summary of care can be sent, to searching for the electronic service information of all participants that support patient discovery and document query to locate critical information about a patient. Resource location is therefore a core functional requirement to support nationwide interoperability.

Recent activity on resource location has focused primarily on directories of Direct addresses (so-called "provider directories") that may include information about organizations and the individuals who are part of each organization. However, there are a number of standards that have been developed and implemented to support resource location beyond Direct addresses in healthcare. For example, the eHealth Exchange specifications use Universal Description Discovery and Integration (UDDI) as the method to search and retrieve information about organizations, including how to perform patient discovery, query for documents, retrieve documents and submit documents. Additionally, IHE created and maintains three profiles for standards-based healthcare-related directories including the Personnel White Pages (PWP) profile[74], the Care Services Directory (CSD) profile[75] and the Healthcare Provider Directory (HPD) profile[76]. The profile receiving the most industry attention, including among eHealth

---

[74] http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf
[75] http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_CSD.pdf

[76] http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_HPD.pdf

Exchange, is Healthcare Provider Directory (HPD) which provides mechanisms to locate individuals and organizations, the relationships between them and Direct addresses or electronic service information.

The EHR│HIE Interoperability Work Group (IWG) created a significant extension to the HPD standard including the creation of additional objects in the HPD Lightweight Directory Access Protocol (LDAP)-based data model to support organizations, sub-organizations, relationships among them and the electronic services they offer. Early in 2013, ONC launched a ModSpec project to produce a testable set of requirements and funded the Exemplar HIE Governance Program to pilot test HPD+ and a new specification resulting from the ModSpec efforts. The pilot had four significant findings:

1. The multitude of HPD standards and implementation guides has resulted in an incompatible set of provider directory deployments across the country.
2. The use of different provider specialty nomenclatures in different provider directories could affect interoperability between directories.
3. There was broad agreement that the new ModSpec specifications needed to go through the IHE approval process, in order to ensure widespread vendor acceptance.
4. The scope of all of the published implementation guides for provider directories did not include federation, nor any guidance regarding harmonization across an environment involving multiple provider directories.

After the pilots, ONC worked with IHE to update the HPD specification and include an optional extension to support federation. The IHE HPD implementation guide was released in October 2014 and can currently be tested on ONC's Standards Implementation & Testing Environment site.[77] The HPD standard may have limitations, particularly as it was built as a directory of individuals and organizations, not services or even Direct addresses. It can be used to discover electronic services, but may not be efficient or flexible enough for the future needs of a learning health system. For example, it can easily hold a URL, but perhaps not the WSDL or content constraints, and therefore does not completely describe the API.

Finally, the CSD profile has been on IHE's planning Roadmap to move beyond HPD. Unlike HPD, CSD was intended as a way to discover services for individuals and organizations. Services in CSD include both clinical services ("what dermatologists are there within 10 miles of my home and when are they available for an appointment"), as well as technical or electronic services ("what is the service for discovering patients at Private Dermatology Specialists where Dr. Smith practices"). A portion of the CSD standard includes busy status and therefore it supports scheduling. CSD has similar data elements as the current version of HPD, but a different architecture. It is not based on LDAP but it does have a federation model that is part of the profile. It can represent individuals and organizations, their relationships and clinical and electronic services associated with those relationships. CSD is a new standard, just approved for test implementation in 2014. As such, it is not yet clear whether CSD will be better suited to support the type of resource location necessary in a learning health system.

---

[77] www.sitenv.org

There are also nationwide directories available that are expanding their services. For example, the Centers for Medicare & Medicaid Services (CMS) is working to improve the accessibility, usability and data quality of the National Plan and Provider Enumeration System (NPPES.) NPPES is the National Enumeration System responsible for assigning the National Provider Identifier (NPI) as mandated by HIPAA. The NPI is a 10-digit unique identifier, similar to a SSN or Corporate Tax Number, used in most healthcare related transactions such as: enrollment with government and private payers, claims payment, prescriptions and health records management. Currently over 4.2M NPIs have been assigned to health care individuals and organizations. The use of the NPPES database has increased over time. On average more than 2,000 users download the publicly available file each month and over 25,000 new NPIs are registered each month. Now more than ever the NPI is being analyzed by the health industry for additional uses, prompting more data requests from the industry.

Today, key information within NPPES, such as provider's practice addresses, telephone numbers and licensure information may be inaccurate or out-of-date because providers have little incentive to update their records.

Moving Forward

A learning health system will grow and change dramatically, especially during its creation over the next few years, but also throughout its lifetime – adding new participants and changing organizational relationships, adding new services, upgrading or retiring legacy services in favor of new and evolving standards, adding new functions, APIs and stakeholders. It is unrealistic to expect any organization to keep track of all of the services available and the API details of each one, even if limited to only those participants and services of interest to them. Resource location acts as a shared directory or collection of directories that allows users and systems in a learning health system to dynamically discover participants of interest and the resources – data and other services – they offer. Due to its dynamic nature, resource location will likely have some degree of decentralized administration in order to operate efficiently and remain accurate and up-to-date.

It will be important that nationwide directories continue to seek out innovative ways in which to maintain the information. For example, the goal of the current CMS project is to improve NPPES data quality using innovative approaches such as:

- **Expanding Relevant Data:** Inclusion of additional optional information such as Direct addresses, web address and multiple practice locations.
- **Expanding Data Accessibility:** Creation of RESTFul web services (APIs) for accessing public information that will allows system to system connectivity and make the NPPES data easier to use by both the public and internal resource for HHS and CMS.
- **Review and Notification:** Regular review and comparison of information against other available records and then notification to providers to verify the information on file.
- **Delegation of Authority:** Enabling others to who have been given permission the ability to update and manage NPPES records on provider's behalf.
- **Reduce Duplicate Data Entry:** Allowing for two-way sharing of data between NPPES and other CMS system such as PECOS, the provider enrollment system for Medicare.

Importantly, resource location will not be responsible for locating health information associated with a patient, condition, or participant. Instead, it provides a means for discovering the services that participants offer and the APIs that can be used to locate health information associated with a patient, condition, or participant. However, many aspects of resource location will be automated to work with the other functionalities described in the Roadmap so that the users of health IT systems will not have to do separate queries for patients and their data, for example.

Since resource location provides a user or system with the tools to access other systems, it will be important to carefully consider security controls and a user's level of access based on their authentication to search the shared directory of participants and resources. As the capabilities of a learning health system expand and more participants join and offer data resources and other services, it will be increasingly important to carefully consider the API used to access it. There are a number of questions that must be addressed in the three- to six-year timeframe, including:

- How does an individual or system place a query to discover participants of a learning health system or the services they offer? How is API information passed back? How does one know that the response is complete?
- How does an individual or system gain access to resource location? How is one authenticated to access the system?
- How is information in resource location managed and updated and how is the information curated to ensure accuracy?

The answers to these questions will help define an architecture for resource location, identify the technical standards that will be used to implement it and the security model to protect its information and determine whether any current capabilities can be leveraged. The resources that need to be coordinated by resource location services include at least the mechanisms to access data repositories, networks and services and APIs.

Ultimately, resource location services will need to have the ability to locate all of these resources in a seamless way, including emerging directories of new participants and services. Additionally, a learning health system will significantly expand the type of participants that may query resource location services, including, but not limited to, individuals/consumers (those that want access or want to facilitate exchange), providers and their systems, payers and their systems and other stakeholders such as schools, prison systems and research organizations.

Table 14: Critical Actions for Reliable Resource Location

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
N1. Development of New Architecture and Standards	1. Through coordinated governance, public and private stakeholders should identify the architecture and workflow for resource location as part of a learning health system, including the individual and IT system actors, roles and access requirements. 2. Through coordinated governance, public and private stakeholders should prioritize the participants and services that are to be discoverable using resource location and identify a near-term goal for the first small set of resources to be included in an initial implementation. 3. From the architecture, SDOs and health IT developers should determine or develop standard(s) and API(s) for discovering participants and resources (including other directories if the architecture is federated), determine whether any of the current standards or legacy services already incorporated in products can be used or extended and develop a Roadmap to implementation of new standard(s) and API(s), if necessary. 4. Through coordinated governance, public and private stakeholders should identify rules of the road for participating in distributed management of resource location, if appropriate for the architecture and actors. This includes establishing policies and procedures for operation of resource location services, including curation of directory information to maintain data quality. 5. Through coordinated governance, public and private stakeholders should work with SDOs and health IT developers to demonstrate standard(s) and API(s) in a trial implementation, beginning with the prioritized set of resources. 6. Through coordinated governance, public and private stakeholders should develop a glide path for moving from current provider directories to future resource location techniques.	7. Stakeholder input requested	8. Stakeholder input requested

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
N2. Refinement and Adoption of Standards and Best Practices	1. As an interim step, ONC will work with others to encourage initial uptake of current provider directory activities 2. ONC will recommend to CMS that NPPES implement support for the provider directory information query API and data model as specified in the IHE HPD Profile. CMS should maintain Direct addresses and ESI in NPPES 3. CMS/HRSA/OIG should advance the proposed effort to consolidate/synchronize national credentialing support systems 4. ONC and other certification bodies will determine how to support provider directories through certification processes 5. ONC will lead the effort to coordinate across federal agencies on the use of existing standards (e.g. provider directory standards) 6. ONC will support testing through its Standards Implementation and Testing Environment (www.sitenv.org)	7. Through coordinated governance, public and private stakeholders should adopt national standards for locating participants and resources. 8. Through coordinated governance, public and private stakeholders should adopt guidance on data quality, maintenance and update processes. 9. Through coordinated governance, public and private stakeholders should work with health IT developers to identify and publish best practices for resource location operational issues that could include data quality, maintenance and update processes.	10. Stakeholder input requested

Tracking Progress and Measuring Success

Why Monitor Progress toward Success?

As the nation moves towards nationwide interoperability, it is important to know where we as collective stakeholders are starting from, how we are progressing and whether or not we have met important milestones toward reaching our goals. Measuring and evaluating national progress can facilitate the identification of specific gaps that the Roadmap will need to address in the future and provide insight into whether the Roadmap's approaches are working. This will enable ONC to work with stakeholders at all levels to redefine strategies and make course corrections as needed.

Call to Action on Measurement and Evaluation of Exchange and Interoperability

ONC has taken a leading role in measuring and reporting on national progress related to health IT adoption and use. ONC will continue to support and coordinate data collection with federal partners related to exchange and interoperability. ONC will also analyze and report on national progress through the Health IT Dashboard to rapidly share progress and provide insight into gaps and next steps.[78] Although ONC will play a coordinating leadership role, assessing nationwide progress requires the participation of stakeholders across the ecosystem. Identifying and remediating gaps can only occur through comprehensive input and monitoring. Measuring progress affects diverse individuals and entities, such as end-users (e.g., providers, individuals), entities enabling exchange and payers, amongst others.

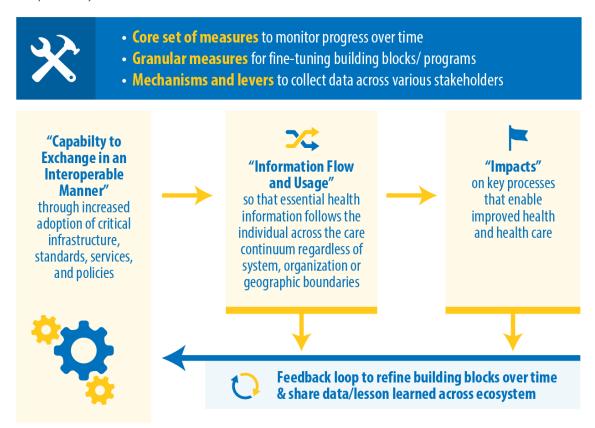## Measurement and Evaluation Proposed Framework: Defining Success

The measurement and evaluation proposed framework identifies key areas that require ongoing measurement (Figure 9). There are three key domains: the adoption of technology and policy enablers that increase the capability to exchange in an interoperable manner; information flow and usage of interoperable information; and, impacts of exchange and interoperability on improved health and health care and the cost of that care. A full description of the domains, including types of measures, is described later in this section.

The framework's scope is for monitoring nationwide progress, which ONC views as distinct from governance monitoring, though there may be overlap in specific measures. ONC plans to monitor a core set of measures across domains; however, by design, the Roadmap's measurement approach is flexible.

---

[78] http://dashboard.healthit.gov/index.php

Mechanisms to collect and disseminate information across stakeholders will be critical to create a transparent system that enables shared lessons and Roadmap refinement.

Figure 9: Measurement and Evaluation Framework for Assessing Nationwide Progress on Exchange & Interoperability

Measuring Success in the Near and Long Term

How success is measured and defined will evolve over time (Figure 10). Expanding the flow and use of essential electronic health information is a near term priority.[79] Initially, ONC will focus measurement on the domains related to interoperable electronic health information exchange capability, information flow and use and to a lesser extent, impacts. Over time, there will be a shift to defining success in terms of how use of information exchanged in interoperable health IT improves outcomes and supports a learning health system.

Figure 10 depicts the *overarching goals and objectives for the next 10 years for expanding interoperable health IT infrastructure.*[80]

---

[79] Connecting Health and Care for the Nation: A 10-Year Vision Paper to Achieve an Interoperable Health IT Infrastructure. ONC. http://www.healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf
[80] Ibid.

Figure 10: 10-Year Overarching Goals and Objectives for Expanding Interoperable Health IT Infrastructure

3 Year Agenda (2015-2017)
Send, receive, find and use a common clinical data set to improve health and health care quality

6 Year Agenda (2018-2020)
Expand interoperable health IT and users to improve health and lower cost

10 Year Agenda (2021-2024)
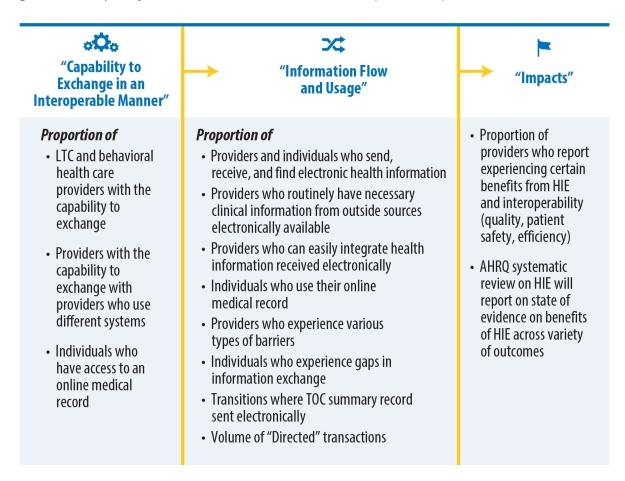Achieve a nationwide learning health system

In the near-term, measurement will be focused on certain populations, such as office-based physicians, hospitals, individuals and long-term care and behavioral health care providers. This reflects available data sources as well as the three-year agenda, which focuses on enabling the sending, finding, receiving and using of essential health information by individuals and providers along the care continuum.[81] Currently available data sources include national surveys of office-based physicians, hospitals, a subset of providers in long-term care settings and individuals, and information reported by program participants, such as the CMS EHR Incentive Programs and DIRECT Trust. Based upon these data sources, examples of specific measures available in 2015-2016 by domain are listed in Figure 11. Over time, the ability to measure success will be more refined and cover a broader ecosystem, as more individuals and providers across the care continuum, including those in non-health care settings (i.e., , long-term services and supports) and public health, share interoperable information and as more data sources become available.

---

[81] Ibid.

"Capability to Exchange in an Interoperable Manner"	"Information Flow and Usage"	"Impacts"
Proportion of • LTC and behavioral health care providers with the capability to exchange • Providers with the capability to exchange with providers who use different systems • Individuals who have access to an online medical record	*Proportion of* • Providers and individuals who send, receive, and find electronic health information • Providers who routinely have necessary clinical information from outside sources electronically available • Providers who can easily integrate health information received electronically • Individuals who use their online medical record • Providers who experience various types of barriers • Individuals who experience gaps in information exchange • Transitions where TOC summary record sent electronically • Volume of "Directed" transactions	• Proportion of providers who report experiencing certain benefits from HIE and interoperability (quality, patient safety, efficiency) • AHRQ systematic review on HIE will report on state of evidence on benefits of HIE across variety of outcomes

Defining Success: Measurement and Evaluation Domains

The next section describes the key domains of the measurement and evaluation framework for tracking national progress. As noted earlier, many of the data sources currently available are largely based upon self-reported data from a subset of providers along the care continuum. Given the limited nature of data sources in the near-term, many of the domains listed in the framework are likely to be measured in the long-term. There are also a number of issues that will need to be considered, including: at what level(s) nationwide measurement should occur (e.g., encounters or patients; users; organizations; or health care system or network-wide) and whether a subset of nationwide core measures should focus on certain subpopulations or use cases where the value of exchanging data using interoperable health IT is and that may be prioritized as part of the Roadmap.

Figure 12: Examples of Measures to Consider for the Long-Term (2017 and beyond)

"Capability to Exchange in an Interoperable Manner"	**"Information Flow and Usage"**	**"Impacts"**
• Adoption of specific technologies, standards, infrastructure and policies to ensure secure exchange of interoperable health IT • Capabilities of providers across care continuum and consumers to securely exchange in an interoperable manner	• Exchange activity • Availability of information to inform decision-making • Usage: rates of accessing available data • Interoperability of data, EHRs and other systems • Uses of interoperable data • Ability to easily integrate data across multiple sources • Reliability, trustworthiness, and utility of information exchanged • Barriers to exchange and interoperability	***Support Key Processes*** • Care delivery and value based payment • Public health surveillance and response • Care coordination and transitions of care across settings • Learning health system and research ***Outcomes*** • Individuals' experience with healthcare delivery system • Reducing costs and increasing efficiency of care • Improving health of populations

Capability to Exchange Through Technology and Policy Enablers

It is essential to ensure that exchange of electronic health information occurs in interoperable health IT across the care continuum and among individuals. Measuring the adoption and implementation of health IT and policy levers will provide insight regarding the extent to which a foundation is in place to support interoperable flow of information. This will involve measuring whether and how interoperable exchange is supported by technology infrastructure, standards, programs and policies. Examples of such measures include: the adoption of "rules of the road" by entities that enable exchange activity, the adoption of best available standards deemed critical to interoperability and exchange, and availability and adoption of key services and/or technology that will enable interoperable exchange. Measuring whether there is the level of interoperability in place to ensure quality measures can be consistently and accurately implemented across various systems, can shed light on the infrastructure and standards that are in place. This might require measuring the adoption and use of "value sets," coded vocabulary groups which incorporate reusable "building blocks" and data elements necessary to calculate clinical quality measures (CQMs). Roadmap milestones associated with the technology and policy enablers will also provide an indicator of progress.

Measuring the Flow and Use of Interoperable Information

Measuring the flow and usage of electronic health information in interoperable health IT is a critical domain in tracking national progress related to the Roadmap. Given that outcome measures may take some time to affect and measure, it will be important to have proxy measures that can be reported in the near-term to refine Roadmap strategies and assess progress. There are several types of measures that assess flow and use of electronic health information shared through interoperable health IT.

Exchange Activity

Measuring exchange activity allows us to assess whether information is flowing in an interoperable manner. Measures of exchange activity should provide insight to:

- **Volume**: whether and how much information is being exchanged;
- **Penetration**: who is exchanging information across the care continuum;
- **Information type**: what types of essential electronic health information are being exchanged and for what purpose or use case;
- **Geographic reach**: where information is exchanged (e.g., nationwide vs. pockets of the country);
- **Organization/System boundaries**: whether and the extent to which information is flowing across systems and organizational boundaries;
- **Exchange mechanisms**: how information is exchanged to identify the services, policies and technologies (e.g., standards, infrastructure) that enable exchange and interoperability including technology infrastructure, standards, programs and policies that support capabilities to engage in interoperable exchange; and
- **Person-Centric**: Exchange occurs when an individual requests it.

Availability and Use of Information from Outside Sources

If information flows in an interoperable manner, information should be available to both providers and individuals when they need it. This might include measuring the availability of information from outside sources at the point of care or the availability of essential electronic health information with online health records for consumers. Measuring actual use of that available information goes a step further towards realizing the full benefits of interoperable health IT. Usage may be measured with simple proxy measures and then evolve to transaction-based measures of accessing or viewing data from outside sources.

Interoperability of Data and Systems

Assessing the extent to which exchanged electronic health information is interoperable is essential so that providers can easily integrate and use information without manual entry. Assessing interoperability will involve measuring whether data sent is received and integrated within interoperable systems. This may vary by information type and by setting, thus granular measurement is required. Interoperability can also be measured through advanced "downstream" uses. An example of downstream use of electronic health information that would demonstrate interoperability includes the incorporation of

data from outside sources for clinical decision support (e.g., ADT alerts). Measuring the ability to easily integrate data from disparate sources, which interoperability of health IT enables, will be important.

Contextual Information

Measuring perceived accuracy, reliability, trustworthiness and utility of information exchanged will help understand variation in use of data. Additionally, information from the end user perspective on barriers to exchange and interoperability may ensure early identification of issues and addressing of concerns.

Measuring and Evaluating Impacts

Data exchanged in interoperable health IT has the potential to support a number of processes to help improve individuals' experiences with the health care delivery system, reducing costs, increasing the efficiency of care and improving the health and wellness of populations. Examples of these processes include: patients' ability to state their privacy choices in an interoperable health IT format as opposed to on paper; care delivery transformation and value based payment models; public health surveillance and response; care coordination and transitions of care across settings; and a learning health system that supports research and scientific discovery.

As progress on interoperability is made, measuring impacts in areas that have shown some promise of being affected by increased use of health information exchange may serve as a way to begin to understand the early effects of expanded interoperability. For example, studies have found that increased use of data exchanged in interoperable health IT is associated with lower readmission rates, decrease rates of admissions from the emergency department to the hospital and lower rates of potentially redundant care.[82,83,84,85,86]

Perhaps in the long-term, national sources of health care utilization data (e.g., Medicare claims data) could be combined with other sources related to health information exchange usage to assess impacts; however, until nationwide data sources on availability and use of health information exchange become a reality, outcomes will largely be assessed through evaluations and research conducted at the local and

---

[82] The potential for community-based health information exchange systems to reduce hospital readmissions. Vest JR, Kern LM, Silver MD, Kaushal R; for the HITEC investigators. J Am Med Inform Assoc. 2014 Aug 6. doi: 10.1136/amiajnl-2014-002760

[83] Association between use of a health information exchange system and hospital admissions. Vest JR, Kern LM, Campion TR Jr, Silver MD, Kaushal R. Appl Clin Inform. 2014 Mar 12;5(1):219-31. doi: 10.4338/ACI-2013-10-RA-0083

[84] The impact of EHR and HIE on reducing avoidable admissions: controlling main differential diagnoses. Ben-Assuli O, Shabtai I, Leshno M. BMC Med Inform Decis Mak. 2013 Apr 17;13:49. doi:10.1186/1472-6947-13-49

[85] Does health information exchange reduce redundant imaging? Evidence from emergency departments. Lammers EJ, Adler-Milstein J, Kocher KE. Med Care. 2014 Mar;52(3):227-34. doi: 10.1097/MLR.0000000000000067

[86] The financial impact of health information exchange on emergency department care. Frisse ME, Johnson KB, Nian H, Davison CL, Gadd CS, Unertl KM, Turri PA, Chen Q. J Am Med Inform Assoc. 2012 May-Jun;19(3):328-33. doi: 10.1136/amiajnl-2011-000394

regional level. Providers' and individuals' perceptions regarding benefits and impacts can also shed light on impacts of exchange and interoperability.

Gaps in Measurement

Although ONC has proposed types of measures that would be important to tracking national progress (Figure 12), these measures may be inadequate to fully measure interoperability. A novel set of metrics may need to be developed and tested for nationwide use. After assessing the current landscape to identify potential measures that may be in use, measurement pilots may need to be conducted to develop and test new metrics or test existing metrics used locally to assess scalability. Measures should possess some key characteristics:

- Valued by a broad set of stakeholders;
- Person-centered;
- Can be aggregated to report up at the population level;
- Replicable so that it can be reported at a national-level;
- Easily understood;
- Objectively measurable and quantifiable: doesn't rely on self-report but upon actual evidence of adoption, use and impact (e.g., log audit data);
- Independent of technical architecture and exchange modality;
- Associated with improvements in key outcomes (e.g., reduced readmissions); and
- Identifies important results that can be used to improve health, or that have meaning for individuals about how well the system is moving around the data about them

Stakeholder involvement of entities that enable exchange (health information organizations, HISPs, health IT developers, etc.), payers and providers will be critical to the development and testing of measures.

Gaps in Available Data Sources

As mentioned earlier, national data on exchange and interoperability is available in 2014 that includes: (1) national surveys of office-based physicians, hospitals, individuals and a subset of providers in long-term care settings; and (2) information reported by program participants, such as the CMS EHR Incentive Program and DIRECT Trust. In 2015-2016, this will be supplemented by one-time surveys of long-term care providers and of behavioral health care providers will be conducted by CMS and SAMHSA respectively.

Based upon these available data sources, ONC has identified a number of gaps (Figure 13). To address the measurement gaps, the types of data sources used to report on nationwide progress related to interoperability and exchange need to be broadened. ONC presently is largely reliant on self-reported data from national surveys and program participants.

Figure 13: Gap Analysis: Availability of Data to Report on Types of Measures for Measurement & Evaluation Framework

"Capability to Exchange in an Interoperable Manner"	"Information Flow and Usage"	"Impacts"
• Adoption of specific technologies, standards, infrastructure and policies to ensure secure exchange of interoperable health IT • Capabilities of providers across care continuum and consumers to securely exchange in an interoperable manner	• Exchange activity • Availability of information to inform decision-making • Usage: rates of accessing available data • Interoperability of data, EHRs and other systems • Uses of interoperable data • Ability to easily integrate data across multiple sources • Reliability, trustworthiness, and utility of information exchanged • Barriers to exchange and interoperability	*Support Key Processes* • Care delivery and value based payment • Public health surveillance and response • Care coordination and transitions of care across settings • Learning health system and research *Outcomes* • Individuals' experience with healthcare delivery system • Reducing costs and increasing efficiency of care • Improving health and health care of populations

Legend: Data Availability

Red = Little or no data   Blue = Some Data   Green = More Data

In particular, there is limited information available from key entities that enable exchange and interoperability, such as health information organizations, HISPs and health IT developers. Such entities can provide information on the volume of exchange activity, as well as the availability and usage of exchanged data, based upon transaction data that is reliant on self-reporting. DirectTrust has reported on key metrics related to the volume of exchange activity based upon data provided by its participants.[87] However, they represent a subset of all the exchange activity that is enabled nationwide. Additionally, simple transaction counts need to be supplemented with measures that provide insight into the number of unique patients or encounters affected, or if/how the information was used.

Another major measurement gap relates to standards. Entities that enable exchange and organizations more directly involved in standards development also need to be engaged, so adoption and experience

---

[87] Exemplar Health Information Exchange Governance Entities Program (Program) Funding Opportunity Announcement. http://www.healthit.gov/policy-researchers-implementers/exemplar-hie-governance-entities-program

with implementing standards can be tracked. ONC to date has focused its measurement on providers along the care continuum and will need to identify data sources to include non-health care settings. Bridging these gaps will be critical to assessing long-term success.

Potential Mechanisms to Address Gaps

Federal agencies, such as AHRQ, already support research related to electronic health information exchange and will continue to support research on exchange and interoperability. It will be important for ONC to coordinate with federal research agencies to ensure that this topic remains a priority and is expanded to cover domains suggested in this framework. Future ONC grantees will provide data on the adoption of technology, services and policies that enable exchange and interoperability, as well as on information flow and use.

ONC plans to leverage partnerships with federal agencies on reporting and tracking. For example, in the *Federal Health IT Strategic Plan 2015-2020*, a number of federal partners have committed to reporting on interoperability. ONC has also developed collaborations with the Federal Trade Commission (FTC) to identify market barriers to exchange and interoperability, promoting healthy competition in health IT markets.[88] ONC will want to leverage other externally available data; examples include nationwide surveys of health information organizations to monitor infrastructure to support exchange and exchange activity.[89] Where data sources are lacking, ONC may need to commission market reports on topics such as the adoption and implementation of standards.

Regulatory or policy levers that would require reporting of key metrics may be necessary in order to obtain national data. Reporting of certain measures as part of governance-related "rules of the road,' the certification process or as part of Meaningful Use reporting requirements would enable nationwide collection and reporting of data for the purposes of monitoring of progress.

---

[88] Tara Isa Koslov. http://www.ftc.gov/news-events/blogs/competition-matters/2014/10/promoting-healthy-competition-health-it-markets
[89] Operational health information exchanges show substantial growth, but long-term funding remains a concern. Adler-Milstein J, Bates DW, Jha AK. Health Aff (Millwood). 2013 Aug;32(8):1486-92. doi: 10.1377/hlthaff.2013.0124

Measurement Actions

Table 15: Measurement Actions

2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
1. ONC, after soliciting feedback from stakeholders and the public, will update measurement strategy to reflect feedback and determine a core set of measures that will be used to track progress over the short-term. 2. ONC will provide baselines and targets for available measures on the ONC Health IT Dashboard and through other vehicles to broadly disseminate the information. 3. ONC will analyze and report on nationwide progress on a regular basis through Congressional reports on health IT adoption and other mechanisms on the ONC Health IT Dashboard. 4. Data holders, entities that enable exchange and other key stakeholders will work with ONC to identify mechanism for reporting of key metrics, including potentially voluntarily publicly reporting at an aggregate level metrics related to exchange activity (e.g., volume and nature of exchange occurring). 5. **ONC will work with relevant grantees to report on key metrics related to exchange and use of data through interoperable health IT and potentially use grantees as a means to develop and test novel metrics.** 6. **ONC will solicit input from external stakeholders on specific identified gaps related to measurement, such as standards and pursue various mechanisms to address gaps**. 7. ONC will conduct a review of alternative, novel metrics in use at the local or regional level that could be used at the nationwide level and assess options to pilot test novel metrics. 8. Federal department and agencies that have committed to reporting on progress related to interoperability for the *Federal Health IT Strategic Plan 2015-2020* will report on measures or milestones annually through the Federal Health IT Advisory Council. 9. After soliciting input from stakeholders, ONC will refine and determine a broader list of measures for longer-term measurement. 10. **ONC, federal partners and governance bodies will coordinate national measurement efforts in order to ensure alignment**. 11. ONC and governance entity (ies) will work together to ensure that key metrics are included as part of governance monitoring or 'rules of the road'. 12. ONC will coordinate with other federal research agencies, states and external funders of research on conducting studies to assess impacts of greater flow and usage of data exchanged using interoperable health IT.	1. ONC will continue to review and update measurement and evaluation framework to assess that the measures correspond with the Roadmaps' evolving approach and shift towards greater outcomes measurement. 2. ONC will implement metrics successfully tested through pilots. 3. ONC will work with federal partners and other stakeholders to incorporate measurement of other providers and entities along care continuum in non-health care settings and other sources. 4. ONC will provide updated set of baselines and targets for new measures on the ONC Health IT dashboard and through other vehicles to broadly disseminate the information. 5. ONC will coordinate with other federal partners to support conducting systematic reviews on the impacts of exchange and interoperability (an update to the systematic review underway at AHRQ) and other mechanisms to generate lessons learned and impacts from greater interoperability. 6. ONC will continue to analyze and report on nationwide progress on a regular basis through Congressional reports on health IT adoption and other mechanisms, such as visualizations on the ONC Health IT Dashboard. 7. ONC will continue to address remaining gaps in conjunction with external stakeholders and other federal partners. 8. Federal departments and agencies that have committed to reporting on progress related to interoperability for the *Federal Health IT Strategic Plan 2015-2020* will continue to report on measures or milestones annually through the Federal Health IT Advisory Council.	1. ONC will continue to review and update measurement and evaluation framework to assess that the measures correspond with the Roadmaps' evolving approach and shift towards greater outcomes measurement and supporting the development of a learning health system. 2. ONC will provide updated set of baselines and targets for new measures on the ONC Health IT dashboard and through other vehicles to broadly disseminate the information. 3. ONC will explore reporting nationwide progress based upon other data sources that will become available due to greater interoperability. 4. ONC will continue to coordinate with other federal partners to support conducting systematic reviews on the impacts of exchange and interoperability (an update to the systematic review underway at AHRQ) and other mechanisms to generate lessons learned and impacts from greater interoperability. 5. ONC will continue to analyze and report on nationwide progress on a regular basis through Congressional reports on health IT adoption and other mechanisms on the ONC Health IT Dashboard.

Appendix A: Background Information on Policy Levers

Federal Agencies

HIE Elements in Public Value-Based Payment Models

Value-based payment programs established under the Affordable Care Act have already begun to create the incentives for interoperability and information exchange across the care continuum. Under the Center for Medicare and Medicaid Innovation, HHS continues to expand its portfolio supporting new approaches to care delivery. Accountable care models, which encourage doctors and hospitals to reduce the total cost of care for patients in exchange for an opportunity to share in savings, are designed to reward more effective care coordination. More than 400 Medicare Accountable Care Organizations (ACOs) have been established in 47 states, serving over 7.8 million Medicare beneficiaries, through the Medicare Shared Savings Program, Pioneer ACO program and other initiatives. Another promising model, the Comprehensive Primary Care Initiative, provides funding for advanced primary care approaches, as well as an opportunity to share in savings with both public and commercial payers, in seven markets across the country.

The parameters of federal value-based payment models offer a number of opportunities to reinforce the adoption of health information exchange capabilities and HIT tools that are instrumental to providers succeeding within these models. Initially, value-based payment models can incentivize or require basic adoption of certified HIT, for instance, requiring a certain percentage of participating providers to have attested for meaningful use stage 1 (e.g., CMMI's Pioneer ACO program), or including HIT adoption as part of the quality measurement framework for a given program (e.g., the Medicare Shared Savings Program). As providers become more sophisticated, HHS can consider transitioning requirements to other measures that reflect interoperability capabilities, such as measures of care coordination. These models, in addition to existing efforts to increasingly tie fee for service payment to quality and value, present a natural pathway to ensure that incentives for interoperability gradually reach larger populations of patients and providers.

In addition to launching new value based payment models for testing, HHS will seek to adopt existing models that have demonstrated value as part of permanent Medicare and Medicaid policy, with the opportunity to codify program design elements around interoperability similar to the requirement for summary record exchange and use of certified health IT for reimbursement under Medicare Part B for chronic care management. The Department of Health and Human Services has set a goal of having 30% of Medicare health care reimbursements through alternative, value based payment models by the end of 2016 and 50% of Medicare health care reimbursements in alternate payment models by the end of 2018. HHS has developed an approach that it believes will achieve these goals, including action steps outlined in this Roadmap to advance interoperability.

Linking HIE to Conditions of Participation for Payment Programs

The federal government sets extensive requirements for organizations paid under the Medicare program that address core quality and safety expectations for any organization participating in the program. Ultimately, as electronic, interoperable exchange of health information becomes more ubiquitous, conditions of participation required for Medicare could be linked to electronic processes when consistent with clinical and safety statutory requirements. For instance, electronic sharing of summary care records between hospitals, skilled nursing facilities (SNFs) and home health agencies could be established as the routine standard for transmitting the information these facilities are required to share across care settings.

Federal Health Plan Contracting

A number of federal government agencies contract directly with health plans to care for employees and other beneficiaries. The Federal Employee Health Benefits program, administered by the Office of Personnel Management, contracts with health plans covering 8 million federal employees and their dependents. Tricare, the health program covering active duty military service members, also contracts with plans to provide out of network care for beneficiaries. Finally, the Department of Veterans Affairs contracts with plans providing out-of-network care as well. In their role as large purchasers of health care, these agencies have a significant opportunity to encourage exchange of health information across their provider networks.

Aligning Federal Contracting Guidelines

In addition to health plans, federal contracts and grants often support acquisition of HIT infrastructure and services across a wide range of agencies. HHS can work with selected agencies to ensure funding streams for capital investments for health information systems include consistent requirements around interoperability standards that all systems must meet. For instance, HRSA investments in health center controlled networks would require health IT acquisitions to comply with specified standards.

States

State Innovation Models Funding

CMS is supporting delivery system and payment reform through Medicaid policies and through the State Innovation Models (SIM) initiative. Including the Round Two awardees and six Round One Model Test states, now over half of states representing 61 percent of the U.S. population (38 total SIM awardees, including 34 states, three territories and the District of Columbia) will be working on efforts to support comprehensive state-based innovation in health system transformation. As part of their SIM approaches, states can leverage federal funding to advance interoperability across the care continuum. For example, Minnesota's and Maine's State Innovation Model work includes financial incentives for health IT adoption and/or technical assistance for behavioral health providers.

Medicaid Managed Care

Medicaid managed care plans also offer significant opportunities for states to advance interoperability. Currently, 41 states and the District of Columbia deliver Medicaid and/or CHIP services through a managed care arrangement. As part of state quality strategies, states can include references to health IT (including EHRs) or health information exchange in any sections that are pertinent to strategic improvement efforts planned by the state, such as identifying enrollees with special needs or health care disparities, collection of data for use in reporting performance measures, use of health IT to assess access, or use of a new health information/exchange technology as an intervention in a performance improvement project or focused study. States can also more aggressively require health information exchange usage as part of managed care organization request for proposals and contracts. A number of these have already made progress with these types of strategies. For instance, Arizona Medicaid requires its managed care health plans through contract to join the state level HIE, while Louisiana's recently launched managed care strategy requires hospitals in participating networks to contribute data to the state health information exchange to support care coordination.

Managed care contracting represents an important lever states can use to require and implement measures and incentives for health information exchange and health IT adoption by providers participating in their programs. HHS could work with states to encourage more widespread inclusion of interoperability elements in these contracts going forward, ensuring provider networks are delivering high quality, safe care to Medicaid beneficiaries across the country through the use of health information exchange.

Section 1115 Waivers

Integration of health information exchange and health IT into state Medicaid programs can also be accomplished under demonstration authority at section 1115 of the Social Security Act (1115 demonstrations). Improved coordination of care through the exchange of health data is a key component that the demonstration programs can leverage and promote commercial health plans' efforts to improve quality of care and health outcomes and lower the growth in costs of health care.[90] In addition, several states are advancing health information exchange in support of payment and delivery reform through Medicaid Delivery System Reform Incentive Payment (DSRIP) programs whereby the state can receive federal financing under a waiver for projects designed to improve access, quality and efficiency in the healthcare delivery system.

State Plan Amendments

States can also use the State Plan Amendment process to integrate health IT and health information exchange within their Medicaid state plans. Several states implementing health homes have done this to ensure health information exchange is enabling care planning and/or care coordination and successful implementation of their programs.

---

[90] For more information, visit Medicaid's website at http://www.medicaid.gov/medicaid-chip-program-information/by-topics/data-and-systems/section-1115-demonstration-hie-policy.html

HITECH Administrative Funding

CMS is able to provide funding for state administrative activities related to core interoperability services (e.g., designing and developing a provider directory, privacy and security applications and/or data warehouses), public health infrastructure, electronic Clinical Quality Measurement (eCQM) infrastructure and provider on-boarding. Funding for interoperability activities is already available to states through the Medicaid EHR Incentive Program. States may request 90/10 HITECH administrative funding for a wide range of interoperability activities that support meaningful use. States can also leverage existing CMS funding authorities to allow patients to download their claims and/or clinical data that are housed in the states' MMIS.

State-Autonomous Levers for Reinforcing Interoperability and Exchange

In addition to leveraging federal funding, states can use independent authorities in a variety of ways to drive interoperability, including: using state-level policy and programs to create a more supportive business environment for interoperability, operating health information exchange services directly according to standards-based approaches (as either an HIE or health care provider) and taking advantage of convening powers to encourage interoperability across state-level stakeholders.

State Policy and Programs

For the purposes of the Roadmap, state policy generally means state laws or state regulations and state programs (again, outside of Medicaid) that direct the spending of state money on providing care or influencing it in some way. The following represent examples of health IT-specific policy and programmatic levers that states are currently employing or have proposed in support of exchange and interoperability:

- **Mandated connection to health information exchange.** Currently states such as Maryland, North Carolina and Vermont all have some form of mandated HIE connection.
- **State-level, standards-based interoperability requirements.** Minnesota law dictates that hospitals and care providers have an "interoperable electronic health records system."
- **Specific health IT mandates** (e.g., eRx or electronic lab exchange). Minnesota passed an e-prescribing mandate in 2011.
- **Creation of a dedicated state fund for health IT** financed through claims transaction fees or other mechanisms. Vermont currently assesses a fee (2/10ths of 1%) on health insurance claims for a state fund to support health IT and health information exchange.
- **State-driven health IT adoption support.** The state of North Dakota created a loan program for providers in the state to adopt health IT.
- **Leveraging health IT infrastructure for other uses within health care and beyond.** This may include alignment with states' Health Benefits Exchanges, advanced directives registries, PDMPs, non-health programs like Supplemental Nutrition Assistance Program enrollment and existing provider directories. One example of this is Maryland's health information organization (the Chesapeake Regional Information System for our Patients), which has partnered with the state

Health Benefits Exchange to create a provider directory for patients to look up whether their providers accept certain insurance.

- **Leveraging state employee benefit requirements.** For example, the state of Arkansas has partnered with the Employee Benefits Division of the Arkansas Department of Finance and Administration to encourage the use of its state health information organization with all of its affiliated providers. Local governments also can take steps to leverage their purchasing power to reinforce interoperability.
- **Requiring health information exchange infrastructure as a public health conduit.** For example, in Alaska, all public health Meaningful Use measures must be submitted through the State health information organization.
- **Removing barriers to exchange through revised privacy and security policies.** Arizona, for example, passed two legislative packages in 2011 and 2012 affecting the state's consent policy and the state's notice of Health Information Practices to patients.

Operating Health Information Exchange Services

States can play a major role in driving interoperability when they directly operate exchange services or designate a third party to do so. While a number of states directly control the operations of a statewide health information exchange itself, others may develop exchange infrastructure to help coordinate care and share information across specific providers where the state has a significant interest, such as public health providers.

States directly enable interoperability when operating or establishing a third party to become a health information exchange entity. They can choose the architecture of their approach, which includes such decisions as what providers focus their connectivity efforts on, whether and how to allow for patient access, and even the standards they use for storing and transporting data. This role also allows states to determine fee structures for their services, which have major impacts on interoperability and exchange. Perhaps most importantly, states that are operating exchange entities also control the governance/oversight of exchange activities. States can also take steps to ensure connectivity for providers ineligible for Meaningful Use. For example, Florida funded a survey of the perceptions of health information exchange by behavioral health centers.

States as Conveners

States have also had success in driving interoperability via their role as conveners, outside of the state's exchange oversight roles. This is important in the context of states' activities related to multi-payer alignment as part of delivery system reform efforts. Such convening may not directly consider exchange, but nevertheless has significant direct impacts on exchange across a variety of stakeholders.

Convening can include broad-based listening sessions as a precursor to concrete planning activities. For example, the State of Vermont conducted public listening sessions related to health IT as part of the creation of the state's Blueprint for Health. It can also mean strategy sessions in pursuit of a particular goal such as the State of Michigan holding meetings to support its efforts to become a Learning Health State. Ultimately, states could create their own interoperability roadmaps.

Private Payers

Value-based payment programs

Private payers have significant opportunities to advance interoperability within value-based payment arrangements they develop with providers. For instance, payers can make adoption of certified health IT systems or demonstration of interoperability a condition of participation for providers that wish to take part in these programs. In markets with more advanced infrastructure for health information exchange, such as an active HIE, payers can consider partnering with the HIE and requiring participation by providers seeking to join these programs.

Within entry-level pay for value and pay for performance programs with individual practices, payers can make use of certified health IT a condition, or link payments to other programs referencing IT requirements, such as medical home certification. Private plans can mirror Medicare policy to support chronic care management and require use of certified health IT. Payers can also include these requirements within more sophisticated arrangements, such as accountable care contracts covering commercial populations, in which groups of providers share in savings generated from more efficient care.

For private payers, these requirements help to ensure that participating providers are able to succeed within value-based payment programs through access to infrastructure that can support robust care coordination across settings of care and reduce unnecessary spending. Payers can also benefit from electronic reporting capabilities associated with use of interoperable health IT to streamline program administration.

Incentivizing Consumers

Private payers also have opportunities to advance consumer demand for interoperability by incentivizing consumers to choose providers that have advanced IT-enabled capabilities around care coordination. Today, payers are increasingly seeking to drive consumers to those providers that have a record of offering high-value, high-quality services. Payers can expand the parameters for high-value providers to take into account use of certified health IT, participation in a health information exchange or other indicator of advanced capabilities. Accordingly, consumers would receive a small incentive to choose these providers, such as lower copays.

Interoperability Requirements for Credentialing

Much in the same way that public payers could eventually include interoperability as part of the basic standard of care delivered by providers paid under public programs, commercial payers can also explore adding health IT and interoperability requirements to the factors included as part of credentialing processes for providers in their networks. If information regarding health IT capabilities were included as a standard component of credentialing information, payers could determine how to give preference to these attributes when identifying their networks.

Alignment for Value-Based Payment

To truly improve care across their patient populations, providers need access to information on patients' total cost of care across payers. Moreover, providers face considerable administrative burden related to managing multiple value-based programs that may have unique incentive and measurement requirements. To support greater alignment across payers, value-based payment models with multi-payer elements, such as the Comprehensive Primary Care Initiative, are providing an important Roadmap for public and private payers to work together.

Alignment of private payer efforts with CMS policies and programs, including incentives for health information exchange and e-clinical quality measures, will enable the three- and six-year goals in the Roadmap. In 2015, CMS intends to support a public-private partnership to increase alignment of key value based payment model attributes among payers and purchasers to facilitate adoption of payment reform goals. This partnership will provide a venue to collaborate across sectors and disseminate best practices and policies that could facilitate broader exchange of common clinical information to support care coordination across the care continuum.

Appendix B: Background Information on Efforts to Promote Individuals' Engagement With Their Health and Health Care

Over the last few years, ONC, CMS and other stakeholders have implemented a number of policies and programs to promote individual engagement with their health care. These activities are described in detail below.

Meaningful Use Stage 2

One objective of Meaningful Use Stage 2 regulations is to provide patients with the ability to view online, download and transmit (VDT) their health information within four business days of the information being available to the Eligible Professional (EP). On the inpatient side, eligible hospitals are required to provide patients the ability to view online, download and transmit information within 36 hours of discharge. Providing patients with an electronic copy of their health information helps them and their caregivers have the information they need to engage more in their care and enables them to identify potential errors or omissions in their records. In addition, having information readily available is useful when patients change providers, seek a second opinion, or are seeing multiple providers during the same time period. They have the ability to share their health information to make sure everyone is on the same page to support care coordination and self-management. This is increasingly important given that one in three individuals reported experiencing one or more gaps in health information exchange within the past year. Even as electronic health information exchange becomes more prevalent, consumers will play an important role managing their own and their loved ones' health information.

Blue Button

Through the public-private Blue Button Initiative,[91] ONC and its supporters are increasing individuals' electronic access to their clinical and claims-related health information from diverse sources. The voluntary Blue Button Pledge program has over 500 organizations, including federal agencies, healthcare provider systems, health insurance plans, labs, retail pharmacies and others who have committed to enabling consumer access to their online health data or to getting the word out to fuel more consumer awareness and demand for access to their digital health data. In 2013, ONC convened focus groups, did consumer testing and developed a set of public service announcement (PSA) videos and posters about Blue Button, customized to three diverse population groups and secured commitments from influential organizations to distribute these materials in 2014 via an ongoing national Blue Button Campaign.[92]

---

[91] www.HealthIT.gov/bluebutton
[92] http://www.healthit.gov/buzz-blog/consumer/launching-fall-national-blue-button-consumer-campaign/

ONC also worked closely with the public to outline the technical standards supporting the ability for consumers to access their health information and for data holders and developers to go a step further and allow consumers to move their data from provider systems to the tools and services they designate. These standards and guidance can be found in the Blue Button Toolkit, formerly known as Blue Button +. ONC has also seeded competitions to help spur the development of consumer-friendly health applications that are able to ingest structured health data from traditional EHR systems. The Blue Button Co-Design Challenge,[93] for example, has led to the development of seventeen consumer apps that accept Blue Button structured data.

Consumer eHealth Program

Through its Office of Consumer eHealth (OCeH), ONC catalyzes, coordinates and inspires others to support consumer engagement via eHealth by influencing policy and standards development, convening diverse stakeholders, building public-private partnerships and providing thought leadership through writing and public speaking. OCeH's efforts span its "three A's" strategy for consumer engagement via eHealth: increase people's *access* to their own digital health information; ensure that information is *actionable* via apps and tools; and promote a change in *attitudes* regarding traditional consumer and provider roles. OCeH works closely with several other offices at ONC (including the Office of Policy and Planning), federal partners and members of the private sector on a variety of activities to advance consumer engagement priorities. OCeH works to integrate the consumer voice across ONC, to make sure that policies, standards, definitions, certification and privacy work relate to both patients and providers.

Federal Advisory Committee Workgroups

Two workgroups made up of volunteer subject matter experts, the HIT Policy Committee's (HITPC's) Consumer Empowerment Workgroup and the HIT Standards Committee's (HITSC's) Consumer Technology Workgroup, issued joint recommendations to the two committees in 2014 about how to support the use of patient-generated health data in the next stage of meaningful use of EHRs. A third workgroup, the HITPC Accountable Care Workgroup, plans to consider how to increase patient activation as a member of a defined care team, engage patients in assessments of their health and use technology to deliver care to patients outside of traditional care settings.

Investing in Innovation (i2) Program

ONC created the Investing in Innovation (i2) program to award prizes competitively to stimulate innovation. The competitions offered by this program, also referred to as health IT developer challenges, focus on innovations that support the following: 1) the goals of HITECH and clearing hurdles related to the achievement of widespread health IT adoption and meaningful use; 2) ONC's and HHS' programs and programmatic goals; and 3) the achievement of a nationwide learning health system that improves

---

[93] http://www.healthit.gov/buzz-blog/health-innovation/onc-announces-winners-blue-button-challenge/

quality, safety and/or efficiency of health care. Through the challenges, ONC has spurred industry innovation in Consumer eHealth, including the development of apps that use Blue Button + structured data, of which there are now more than 17. The program also hosted a Blue Button Design Challenge in 2013 to challenge designers across the country to reimagine the patient health record.

VA's Innovation Program

The US Department of Veterans Affairs manages the VA Center for Innovation that includes an Industry Innovation Competition. The VA Center for Innovation identifies, tests and evaluates new approaches to efficiently and effectively meet the current and future needs of veterans through innovations rooted in data, design-thinking and agile development. It has been in existence since 2010 with over 18,000 ideas submitted and numerous innovations that have led to improvements at the VA.
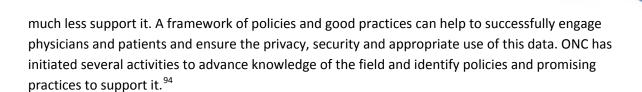
Care Planning

As the capabilities of health IT tools increase and a national infrastructure for electronically sharing health information becomes more ubiquitous, individuals and stakeholders across the care continuum are converging around a vision where a single care plan can be captured, dynamically updated and utilized in a secure and appropriate fashion by individuals, caregivers and any member of the individual's virtual, interdisciplinary care team. A range of program requirements within Medicare and Medicaid and other federal programs indicate that participating clinicians must develop care plans as part of their services for beneficiaries.

New initiatives continue to emphasize the importance of care management program in the Physician Fee Schedule. In addition, payment reform models being advanced at the local, state and federal levels are increasingly pointing to care plans as a way to support needed care coordination, quality improvement and cost reductions. Finally, care coordination has been established as one of the six priorities of the National Quality Strategy developed under the Affordable Care Act; effective shared care planning across institutions is widely acknowledged as one of the key tools for achieving more robust care coordination. Through the S&I Longitudinal Work Group, several sites have implemented the pre-ballot C-CDA R2.0 and several organizations demonstrated Care Plan exchange using pre-ballot C-CDA R2.0.

Patient-Generated Health Data

Patient-generated health data are health-related data—including health history, symptoms, biometric data, treatment history, lifestyle choices and other information—that is created, recorded, gathered or inferred by or from patients or their designees (i.e., , care partners or those who assist them). This data is distinct from data generated in clinical settings and through encounters with providers in two important ways. First, patients, not providers, are primarily responsible for capturing or recording these data. Second, patients direct the sharing or distributing of these data to recipients of the individual's choosing, which range from caregivers to health care providers and other stakeholders. There are no widely established policies and practices to define the optimal use of patient generated health data,

much less support it. A framework of policies and good practices can help to successfully engage physicians and patients and ensure the privacy, security and appropriate use of this data. ONC has initiated several activities to advance knowledge of the field and identify policies and promising practices to support it.[94]

Personalized Health Care

While the concept of personalized health care is not new, genomic, proteomic and other discoveries are accelerating the tailoring of patient treatments, risk assessment and diagnostic reasoning. The 2008 publication of the *Priorities for Personalized Medicine* report to the President's Council of Advisors on Science and Technology (PCAST) described personalized medicine as, "the tailoring of medical treatment to the specific characteristics of each patient… [involving]… the ability to classify individuals into subpopulations that are uniquely or disproportionately susceptible to a particular disease or responsive to a specific treatment."[95]

The use of health IT can support shared decision-making and increased communication in clinical practice, helping providers and patients to manage and use patient-specific information. In 2012, ONC conducted some initial research on personalized health care to better understand the current landscape and the definition of the topic. As a result, challenges were identified and health IT-related policy areas are under consideration.

---

[94] http://www.healthit.gov/policy-researchers-implementers/patient-generated-health-data.

[95] http://www.whitehouse.gov/files/documents/ostp/PCAST/pcast_report_v2.pdf

Appendix C: Background Information on Cybersecurity and Encryption

Cybersecurity

There are increasing cyber-attacks on electronic health information, particularly large stores of information. In 1998, Presidential Decision Directive (PDD) 63, acknowledged the need to protect the nation's critical infrastructure from both physical and cyber-attacks.[96] A major outcome of the PDD was the development of Information Sharing and Analysis Centers (ISACs) for each critical infrastructure sector. ISACs are, "privately led sector-specific organizations advancing physical and cyber security critical infrastructure protection by establishing and maintaining collaborative frameworks for operational interaction between and among members and external partners."[97]

One of the goals of an ISAC is to promote and enhance the bi-directional sharing about cyber threats and vulnerabilities within its sector-specific organizations and the federal government. This information sharing advances resilience, which is the ability to prepare for and respond to threats and vulnerabilities within a specific industry. ISACs are currently established for critical infrastructure sectors such as financial services, electricity and water. The National Health ISAC (NH-ISAC) is a non-profit industry-led effort to address the cyber security threats to healthcare and public health. In 2003, the Department of Homeland Security's *Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection*, designated HHS as the Sector-Specific Agency responsible for ensuring the integrity of the health system.[98] A subsequent Presidential Policy Directive identified healthcare and public health (HPH) as a critical infrastructure sector.[99] Despite being identified as critical infrastructure for the nation, healthcare is one of the industry sectors least prepared for a cyber-attack, as it is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures, much less against more advanced persistent threats.[100]

There are various factors within healthcare that contribute to the aforementioned cybersecurity challenge. The health IT ecosystem is composed of multiple systems that are interconnected, including EHRs, laboratory systems, patient portals, medical devices and many other systems. Consequently, the ecosystem is incredibly complex, with these systems being managed across an exponential number of

---

[96] The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. May 22, 1998. http://www.fas.org/irp/offdocs/paper598.htm
[97] NIST Cybersecurity Framework

[98] Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection. December 17, 2003. http://www.dhs.gov/homeland-security-presidential-directive-7
[99] Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. February 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
[100] http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf

organizations. As all of these health IT systems become connected to each other, the cyber threats increase at a significant rate, as an intrusion in one system could allow intrusions in multiple other systems. Additionally, there is high variability in the capabilities and resources healthcare organizations have at their disposal to prevent cyber-attacks. Large organizations have the resources and expertise to have a dedicated information security team to address cybersecurity; however, small and mid-sized organizations may not have these resources and may not be able to afford them. Finally, there is a significant behavioral and cultural change necessary in the industry regarding the relevance of cybersecurity risks. Many in the industry do not realize the significant risk to their systems and do not understand the importance and urgency of implementing security best practices to prevent cyber-attacks.

There are increasing cyber-attacks on electronic health information, particularly large stores of information. Despite being identified as critical infrastructure for the nation, the healthcare system could do more to prepare for a cyber-attack.[101] There are various factors within healthcare that contribute to this aforementioned cybersecurity challenge. The health IT ecosystem is composed of multiple systems that are interconnected, including a wide variety of inputs that need security controls such as EKG machines, EHRs, robots and many other systems. Consequently, the ecosystem is incredibly complex, with these systems being managed across an exponential number of organizations. As all of these health IT systems become connected to each other, security risk can rise, as an intrusion in one system could allow intrusions in multiple other systems.

Additionally, there is high variability in the capabilities and resources that healthcare organizations have deployed to prevent cyber-attacks. Large organizations have the resources and expertise to have a dedicated information security team to address cybersecurity; however, small and mid-sized organizations may not have these resources and some may not be able to afford them. Finally, significant behavioral and cultural changes are necessary in the industry regarding the relevance of cybersecurity risks. Many in healthcare do not realize the significant risk to their systems and do not understand the importance and urgency of implementing security best practices to prevent cyber-attacks.

Encryption

Encryption of data both at rest and in transit is another component of a ubiquitous, secure network infrastructure. Encryption is a method of scrambling or encoding data so that it cannot be read without the appropriate key to unscramble the content. Two common ways encryption is used or applied are to send messages (particularly over networks that are not secure otherwise, like the Internet) and store data. These are sometimes referred to as information in transit and information at rest, respectively. In both cases, the core mechanism is the same. A program takes a piece of information (a string of data bytes) and changes it into another piece of information (a different string of bytes, and not necessarily

---

[101] http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf

the same number of bytes). The original piece of information is commonly referred to as being in the clear and the piece of information into which it is changed is referred to as encrypted. For encryption to work, it must be possible for another program (or possibly another algorithm in the same program) to reverse the process and change the encrypted information back into the information in the clear. This is called decrypting. Another constraint is that the algorithm to decrypt should not be obvious; otherwise, unwanted recipients would be able to recover the original information.

Encryption of data at rest is in some aspects simpler than encryption of data in transit. Data at rest is encrypted and decrypted through capabilities of most major database management systems, most laptop operating systems and at least some mobile operating systems. Encryption of data in transit, however, may require appropriate software compatibility across a learning health system's technology as well as effective management of a public/private key environment.

Encryption technology is not being fully utilized in health care. OCR, in promulgating the breach notification regulations, created a safe harbor for electronic health data that was encrypted such that if that data was accessed, used, or disclosed while encrypted, it did not result in a reportable, remediable breach of ePHI. Despite this safe harbor, health IT systems have been slow to adopt encryption technology, both of data at rest and in transit and the result is that 35% of 2013 breaches reported to HHS were the result of a theft or loss of an unencrypted device containing protected health information.[102]

---

[102] Breach Report 2013: Protected Health Information (PHI). Redspin. February 2014.
https://www.redspin.com/docs/Redspin-2013-Breach-Report-Protected-Health-Information-PHI.pdf

Appendix D: Background Information on Permission to Disclose Identifiable Health Information

HIPAA Privacy Rules

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), a federal law, serves as the foundation for federal protection of the privacy and security of individually identifiable health information. The HIPAA Privacy Rule, adopting principles established in the FIPPs, sets standards governing the use and disclosure of PHI by covered entities (i.e., , health plans including self-insured employer plans and insurance companies, health care clearinghouses and most health care providers – those who transmit any health information in electronic form in connection with specified administrative simplification transactions) and their business associates.[103],[104]

The HITECH Act mandated that the HIPAA Privacy and Security Rules be amended to directly apply parts of the HIPAA Privacy Rule and all of the HIPAA Security Rule to covered entities' business associates (i.e., third parties that perform certain functions or activities on behalf of the covered entity that require the use or disclosure of PHI including, for example, claims processing or data analysis). HIPAA also requires that covered entities supply individuals with a Notice of Privacy Practices, intended to fulfill the fair information practices of transparency and notification.

In general, the Privacy Rule provides that a covered entity may only access, use, or disclose protected health information as permitted or required by the Rule without an individual's written authorization. And it also specifies the circumstance in which the individual's written authorization is required before access to, use, or disclosure of the individually identifiable health information can occur and thus before an electronic exchange of health information (a disclosure) could occur.[105] Of particular importance to a learning health system is the fact that the Privacy Rule permits the use and disclosure of PHI for treatment, payment and health care operations (TPO) without express patient permission (called "consent" in this Road Map and in other venues). Specifically, a covered entity may:

1. Use and disclose PHI for its own TPO activities,
2. Disclose PHI for the treatment activities of any other health care provider (regardless of whether the receiving provider is subject to the Privacy Rule)

---

[103] 45 C.F.R. 160.103.

[104] 45 CFR Parts 160, 162 and 164. Administrative simplification standards include the following transactions: (A) health claims or equivalent encounter information, (B) health claims attachments, (C) enrollment and disenrollment in a health plan, (D) eligibility for a health plan, (E) health care payment and remittance advice, (F) health plan premium payments, (G) first report of injury, (H) health claim status and (I) referral certification and authorization.

[105] 45 C.F.R. §164.502.

3. Disclose PHI for the payment activities of another covered entity and of any health care provider and

4. Disclose PHI for the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the PHI pertains to the relationship. Health Care Operations that meet this category are:

   a. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination; contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

   b. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance; health plan performance; conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers; training of non-health care professionals; accreditation, certification, licensing, or credentialing activities; and

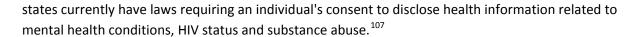   c. Conducting or arranging for fraud and abuse detection and compliance programs.[106]

Under the HIPAA Privacy Rule, an individual's written authorization is not required for the sharing of health information for TPO. Although individual consent is not required, covered entities may (and often do) voluntarily choose to obtain an individual's consent ("basic choice") to use and disclose information about them for TPO.

Additional Requirements for Written Permission

Unlike the HIPAA basic structure, some State and other federal laws and regulations may require an individual's written permission before disclosing particular types of individually identifiable health information. In particular, these limits are found in rules pertaining to "sensitive" health information. Thus, this type of rule may impose additional limitations on the exchange of certain health information. A number of existing federal and state laws impose specific confidentiality requirements on particular types of health information in order to encourage patients to seek treatment (e.g., mental health related information). Some laws require that when sensitive health information is disclosed, the receiving organization be notified that it cannot further disclose the information without obtaining the patient's consent to do so. This restriction is often called a prohibition on re-disclosure. One federal law that has this requirement is 42 U.S.C. § 290dd-2, which protects the confidentiality of information related to substance abuse treatment received through federally assisted programs. For example, many

---

[106] 45 CFR 164.501, 45 CFR 560(c); Disclosure of this type is subject to "necessity;" that is, only the information necessary for the purpose may be accessed, used or disclosed.

states currently have laws requiring an individual's consent to disclose health information related to mental health conditions, HIV status and substance abuse.[107]

Typically, the underlying purpose of these laws is to encourage greater participation and trust in the health care system by protecting a patient's most private and personal health information. The HIPAA Privacy Rule does not preempt these laws that require consent (where HIPAA does not), in part, because they are more protective of privacy than the HIPAA Privacy Rule.[108] Furthermore, in the wake of HITECH, some states also enacted laws to specify that among the conditions for which patient's consent was required was electronic health information exchange,[109] but this type of law has not been enacted in majority of states.

In addition to these laws, some organizations have developed their own internal policies requiring patient consent in order to share particularly sensitive information, or have adopted policies such that non-sensitive information may not be exchanged without a patient's written consent (despite the provisions of the Privacy Rule). Further, many stakeholders believe that individuals should have the ability to control access to the specific health information, or to specify which providers may have electronic access to it.

The preceding paragraphs demonstrate that the U.S. legal, regulatory and policy landscape for sharing health information is complex. While HIPAA sets a "floor" with federal laws and regulations, state laws are often more restrictive than HIPAA and vary from state to state. These variations in state law and variation in policies that organizations voluntarily adopt, make the environment complex.

This complexity hinders interoperability because stakeholders do not have the same standards for determining when patient "consent' is required, or when they may exchange health data without patient consent. Because the stakeholders lack consensus and because the underlying laws and regulations may vary from state-to-state, it is difficult to develop nationwide-technical standards for documenting what access, use or disclosure rule applies and whether, when a patient's consent is legally required, it has been given.

Additional Policy Work on Individual Choice

ONC has received significant advice from federal advisory committees regarding a patient's choice to share his/her PHI. In 2006, the National Committee on Vital and Health Statistics (NVCHS) made a number of recommendations to the Secretary of HHS regarding privacy and the Nationwide Health Information Network (NwHIN), including a specific recommendation that patients be provided with

---

[107] Consumer Partnership for eHealth. Protecting Sensitive Health Information, June 2010, at 2-3. Available at: http://www.nationalpartnership.org/site/DocServer/Sensitive-Data-Final_070710_2.pdf?docID=7041
[108] Health Insurance Portability and Accountability Act of 1996, Pub. Law 104-191, § 1178 (a); 45 C.F.R. § 160.203 (2009).
[109] See NGA Center for Best Practices, State and Federal Consent Laws Affecting Interstate Health Information Exchange, March 2011, http://www.nga.org/files/live/sites/NGA/files/pdf/1103HIECONSENTLAWSREPORT.PDF

choice regarding whether their PHI is accessible via the NwHIN.[110] The NwHIN exchange model was the only one in existence at the time of the NCVHS recommendations. Additionally, NCVHS recommended that HHS evaluate whether a national opt-in or opt-out policy would be appropriate and assess whether individuals should be able to control access to specific content within their health records.

In 2008 and 2010, NCVHS provided further recommendations focused on the exchange of sensitive health information. The recommendations emphasized that the NwHIN should be designed to permit individuals to "sequester," or restrict access to, specific sections of their health record in one or more predefined categories. NCVHS recommended defining this list of potentially sensitive categories and their contents on a national basis in order to achieve greater uniformity. Additionally, the group submitted a number of recommendations related to how these choices should be implemented in practice. For example, NCVHS recommended that where sensitive information has been sequestered, notations in the record transmitted should indicate that the record is not complete and access to the information should be provided in emergency situations.[111]

In 2010, the HITPC held hearings on policies related to patient consent for participating in health information exchange, as well as technological means for implementing consent in an electronic environment.[112] While recognizing the promise of early developments, the HITPC recommended that ONC conduct further research into data segmentation and other such technologies in pilot studies to determine their workability and scalability.[113] "The same considerations and customary practices that apply to paper or fax exchange of patient health information should apply to direct electronic exchange. As always, providers should be prepared and willing to discuss with patients how their information is disclosed; to take into account patients' concerns for privacy; and also ensure the patient understands the information the receiving provider or clinician will likely need in order to provide safe, effective care."[114,115]

Thus, as early as 2010, it was recognized that laws and regulations did not always require patient consent for exchange; instead it was recognized that consent was just one of eight FIPPs. This of course

---

[110] National Committee on Vital and Health Statistics (NCVHS). Letter to the Secretary of Health and Human Services re: Recommendations Regarding Privacy and Confidentiality in the National Health Information Network, June 22, 2006, available at http://ncvhs.us/wp-content/uploads/2014/05/privacyreport0608.pdf.

[111] NCVHS. Letter to the Secretary of Health and Human Services re: Individual Control of Sensitive Health Information via the Nationwide Health Information Network for Purposes of Treatment, February 20, 2008 and NCVHS. Letter to the Secretary of Health and Human Services re: Recommendations Regarding Sensitive Health, November 10, 2010.

[112] http://www.healthit.gov/sites/default/files/archive/index.php?dir=FACA%20Hearings/2010/2010-06-29%20Policy%3A%20Privacy%20%26%20Security%20Tiger%20Team%2C%20Consumer%20Choice%20Technology%20Hearing or http://healthit.gov/archive/?dir=archive_files/FACA%20Hearings/2010

[113] http://www.healthit.gov/facas/sites/faca/files/hitpc_transmittal_p_s_tt_9_1_10_0.pdf

[114] http://www.healthit.gov/facas/health-it-policy-committee/health-it-policy-committee-recommendations-national-coordinator-health-it

[115] http://www.healthit.gov/facas/sites/faca/files/HITPC_Transmittal_08212013.pdf

did not diminish the need for appropriate and interoperable technical standards for adjudicating permission and ensuring that downstream use complies with the permissions ("persistence") throughout the health information system. The HIT Policy Committee recommendations did however, identify that consent was not required by law and regulation for a significant majority of potential healthcare exchange purposes that were not covered by more restrictive state or federal rules and regulations as discussed generally above.

In September 2011, to address these HIT Policy Committee recommendations, ONC funded the Data Segmentation for Privacy (DS4P) Initiative[116] through the S&I Framework. DS4P gathered a community of experts, including software developers, health care providers, patient advocates and health informaticists, to assess health IT data standards and their practicality. Also in 2011, ONC funded the eConsent Trial project to develop and implement electronic and innovative ways to gather patients' input on areas in which they want to learn more about consent, to educate patients in a provider setting about the electronic sharing of their health information through an EHR and to capture and record choices patients make.[117]

In 2012, ONC released guidance for the State Health Information Exchange Cooperative Agreement Program in response to these recommendations regarding individual choice. The guidance included the following: "Where HIE entities serve solely as information conduits for directed exchange of individually identifiable health information (IIHI) and do not access IIHI or use IIHI beyond what is required to encrypt and route it, patient choice is not required beyond existing law. Such sharing of IIHI from one health care provider directly to another is currently within patient expectations. Where HIE entities store, assemble or aggregate IIHI beyond what is required for an initial directed transaction, HIE entities should ensure individuals have meaningful choice regarding whether their IIHI may be exchanged through the HIE entity. This type of exchange will likely occur in a query/response model or where information is aggregated for analytics or reporting purposes."[118]

Also in 2012, ONC, in coordination with the HITPC, issued as Request for Comment (RFC) for meaningful use stage 3 that included questions and considerations regarding patient consent.[119] In 2013, in response to the public comments received regarding the patient consent questions in the meaningful use stage 3 RFC, the HIT Policy Committee referred to its recent recommendations on Query/Response regarding the technical mechanisms to support communication of patient consent requirements.[120]

---

[116] http://www.healthit.gov/providers-professionals/ds4p-initiative

[117] http://www.healthit.gov/providers-professionals/econsent-toolkit

[118] See ONC's Program Instruction Notice (PIN), Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program, March 2012, http://www.healthit.gov/sites/default/files/hie-interoperability/onc-hie-pin-003-final.pdf

[119] http://www.healthit.gov/sites/default/files/hitpc_stage3_rfc_final.pdf

[120] In particular, data holders and requesters should comply with applicable law and policy and should have a technical way to communicate applicable consent or authorization needs and requirements. They should also have a means to maintain a record of such transactions. See, http://www.healthit.gov/FACAS/sites/faca/files/HITPC_Transmittal_08212013.pdf

The HIT Policy Committee recommended that the HIT Standards Committee should further consider technical methods for giving providers the capacity to comply with applicable patient authorization requirements or policies. On the question related to data segmentation, the HIT Policy Committee deferred further discussion on the topic until it receives an update on the DS4P initiative pilot projects.[121] ONC also released the *Principles and Strategy for Accelerating Health Information Exchange,* which noted that HHS will develop standards and policies to enable electronic management of consent and health information exchange among providers treating patients with sensitive health data such as those with behavioral health conditions or HIV.[122]

In 2014, as part of the HHS Secretary's Strategic Initiative focused on privacy,[123] HHS committed to encouraging the development and use of policy and technology to advance patients' rights to access, amend and make choices for the disclosure of their electronic health information. HHS also noted support for the development of standards and technology to facilitate patients' ability to control the disclosure of specific information that is considered by many to be sensitive in nature (such as information related to substance abuse treatment, genetic information, reproductive health, mental health, or HIV) in an electronic environment.[124]

Most recently, the HIT Policy Committee's Privacy and Security Tiger Team revisited the discussion of data segmentation's applicability to behavioral health information and in July 2014, the HIT Policy Committee submitted recommendations to ONC for voluntary EHR certification criteria, contingent on readiness of specific standards that a recipient EHR can receive and automatically recognize documents from Part 2 providers, but the document is sequestered from other EHR data.[125] A recipient provider using DS4P would have the capability to view the restricted C-CDA (or data element), but the C-CDA or data cannot be automatically parsed/consumed into the EHR. Document level tagging can help prevent re-disclosure.

---

[121] http://wiki.siframework.org/Data+Segmentation+for+Privacy+Homepage
[122] Principles and Strategy for Accelerating Health Information Exchange (HIE). ONC. August 2013, http://www.healthit.gov/sites/default/files/acceleratinghieprinciples_strategy.pdf
[123] See U.S. Department of Health and Human Services, HHS Secretary Strategic Initiative: Protect Patients' Health Information and Their Privacy Rights, (March 2014), http://www.hhs.gov/strategic-plan/patient-privacy.html
[124] Ibid.
[125] HITPC Recommendations to ONC, July 2014, http://www.healthit.gov/facas/sites/faca/files/PSTT_DS4P_Transmittal%20Letter_2014-07-03.pdf

Appendix E: Background Information on National Information Exchange Model (NIEM)

National Information Exchange Model

The National Information Exchange Model (NIEM) is a national program to increase information sharing among organizations at the federal, state and local levels. Its Human Services Domain is used increasingly across HHS to help standardize interoperability of human services exchange use cases. The NIEM model is designed for exchanging information between disparate systems without being intrusive to those domains. NIEM is implementation agnostic, meaning it can serve as an overlaying system-to-system exchange model without ever touching or changing the underlying systems' software code or structure. NIEM is focused on the reusability and standardization of its data model: an expansive, carefully curated XML schema. NIEM enables the structured use of standards, documented in an online repository of information exchange package documentations (IEPDs) to support information sharing.

NIEM is increasingly utilized across HHS, with the Agency for Children & Families playing an important leadership role in the NIEM Human Services domain.[126] ONC is the steward of the NIEM Health domain.[127] There are opportunities to extend NIEM's extensive catalog of exchange protocols and procedures to include examples of bi-directional, health care to human services interoperability. States are currently using NIEM to define and pilot State-to-State exchange between PDMP registries. The CMS Federal Hub that authenticates individuals for the CMMI Health Marketplace subsidy and CMCS Medicaid eligibility uses NIEM to document the exchange requirements between the States, CMS, IRS, SSA and DHS.

A multi-pronged approach and engagement on the part of stakeholders across the ecosystem will be required parties to clarify NIEM's potential and to develop and recommend strategies for use of the NIEM model for approaches to health care and human services information sharing. While ONC can assist in the coordination of delivery system reform efforts working on bi-directional health care exchange with human services to encourage collaboration across jurisdictions, states and other stakeholders across the ecosystem will need to play an active role in determining the role of NIEM to support health care and human services interoperability.

A key area of focus for the role of NIEM could be in relation to the Medicaid Information Technology Architecture (MITA) and interoperable exchange between State Medicaid systems and Health Information Exchange organizations. States and others should develop one or more use cases for health care and human services information sharing and produce one or more Information Exchange Package Documentation (IEPD) based on the requirements of evolving accountable, outcomes-focused payment arrangements and delivery system innovations. Such work will form the basis for widespread sharing of

---

[126] https://www.niem.gov/communities/emc/hs/Pages/about-hs.aspx
[127] https://www.niem.gov/communities/emc/health/Pages/about-health.aspx

health and human services that impact health data to support coordination of care and services across the health and human services ecosystem.

Appendix F: Background Information on Medication Use and Management

Medication Use and Management

Use of pharmaceuticals is a mainstay in the delivery of evidence-based medical care. In fact, approximately half of all Americans take a prescription medication each month and in 2010, there were 2.6 billion medications ordered or prescribed.[128] The need remains to build health IT infrastructure that supports both optimal and safe use of pharmaceuticals. There are more than 770,000 injuries and deaths each year due to adverse drug events.[129]

Electronic prescribing (or e-prescribing) refers to the process where a prescriber generates and transmits an "accurate, error-free and understandable" prescription directly to a pharmacy through a secure network.[130,131] With the advent of e-prescribing[132] and associated clinical decision support systems, many of the safety concerns inherent in paper-based prescribing have been eliminated.[133] Despite these advances, the full potential of e-prescribing is yet to be realized. A high quality e-prescribing process can support higher-level functions, such as medication reconciliation and medication adherence.

Apart from the gains in efficiency and safety that e-prescribing allows, the opportunity exists to use these processes to address growing challenges in healthcare, such as the prescription drug abuse epidemic.[134,135,136] Although 49 states now allow electronic prescribing of controlled substances, less

---

[128] CDC. 2014. http://www.cdc.gov/nchs/data/hus/hus13.pdf

[129]Reducing and Preventing Adverse Drug Events to Decrease Hospital Costs, Publication #01-00. Agency for Healthcare Research and Quality (AHRQ). 2001.

[130] CMS. E-prescribing. Available at: http://www.cms.gov/Medicare/E-Health/Eprescribing/index.html?redirect=/eprescribing/. Accessed on: August 8, 2013.

[131] Department of Health and Human Services Health Information Technology and Quality Improvement. How does e-prescribing work? Available at:
http://www.hrsa.gov/healthit/toolbox/HealthITadoptiontoolbox/ElectronicPrescribing/epreswork.html. Accessed on: August 8, 2013.

[132] IOM Committee on Identifying and Preventing Medication Errors. Preventing Medication Errors: Quality Chasm Series. Washington, DC: National Academies Press; 2007

[133] Sirajuddin AM, Osheroff JA, Sittig DF, Chuo J, Velasco F and Collins DA. Implementation Pearls from a New Guidebook on Improving Medication Use and Outcomes with Clinical Decision Support. Effective CDS is Essential for Addressing Healthcare Performance Improvement Imperatives. J Healthc Inf Manag. 2009 Fall; 23(4): 38–45

[134] Fischer MA, Vogeli C, Stedman M, Ferris T, Brookhart MA, Weissman JS. Effect of electronic prescribing with formulary decision support on medication use and cost. Arch Intern Med 2008; 168(22):2433-39.

[135] Fischer MA, Stedman MR, Lii J, Vogeli C, Shrank WH, Brookhart MA et al. Primary medication non-adherence: analysis of 195,930 electronic prescriptions. J Gen Intern Med 2010; 25(4):284-90.

[136] Lapane KL, Rosen RK, Dube C. Perceptions of e-prescribing efficiencies and inefficiencies in ambulatory care. Int J Med Inform 2011; 80(1):39-46.

than 1% of providers are currently sending prescriptions for controlled substances electronically.[137] Ubiquitous use of electronic prescribing of controlled substances will enable healthcare providers, as well as state entities, to better track use of highly addictive medications and deploy appropriate resources and interventions to areas in need. A second component to addressing this epidemic is Prescription Drug Monitoring Programs (PDMPs).

PDMPs are secure state-administered electronic databases that track the prescribing and dispensing of controlled substances and other prescription drugs of concern. PDMPs can be a powerful tool in the hand of healthcare providers. Evidence continues to accumulate that PDMPs are effective in improving clinical decision-making, reducing "doctor shopping" (utilizing more than one prescriber to obtain controlled substance prescriptions) and the diversion of controlled substances and assisting in other efforts to curb the prescription drug abuse epidemic. However, a significant barrier to increased use and interoperability is the lack of standard methods to exchange and integrate data from PDMPs to health IT systems, meaning that accessing PDMP data is not easily integrated into the e-prescribing workflow.

Today, 49 states and one U.S. territory (Guam) currently have a PDMP that is operational (meaning collecting data from dispensers and reporting information from the database to authorized users). Despite progress in making PDMPs operational, efforts are needed to further facilitate the exchange of PDMP data across state lines. Secure and standardized interstate data sharing would allow prescribers full visibility into patient prescription fill patterns and reduce or eliminate doctor and pharmacy shopping that occurs across state lines. As of November 2014, 29 state PDMPs can share data across state lines with other states' databases.

Comprehensive Medication Management (CMM) is a process by which the appropriateness, effectiveness, safety and compliance of pharmaceutical treatments is evaluated. There are four general steps in the process that require involvement of multiple members of the health care team: 1) assessing the patient's medication needs; 2) identifying any medication-related problems; 3) developing a care plan that includes the patient's personalized goals; and 4) monitoring and follow-up to determine and document patient outcomes.[138] There is evidence to suggest that current efforts at practice transformation and care re-design still require additional effort in order to achieve quality benchmarks through optimal medication use.[139]

Pharmacists are health care professionals with skills and expertise that uniquely position them to work with other healthcare providers to successfully manage patient mediation therapies.[140] Pharmacists routinely consult on choice and selection of appropriate medication therapies, evaluate the

---

[137] Gabriel MH, Yang Y, Vaidya V and Wilkins TL. Adoption of Electronic Prescribing for Controlled Substances Among Providers and Pharmacies. Am J Manag Care. 2014;20(11 Spec No. 17):SP541-SP54

[138] Patient Centered Primary Care Collaborative. The Patient-Centered Medical Home: Integrating Comprehensive Medication Management to Optimize Patient Outcomes Resource Guide 2012 2nd Edition.

[139] Dubois RW, Feldman M, Lustig A, Kotzbauer G, Penso J, Pope SD and Westrich MA. Are ACOs Ready to be Accountable for Medication Use?   J Manag Care Pharm. 2014;20(1):17-21.

[140] Joint Commission of Pharmacy Practitioners. Pharmacists Patient Care Process. 2014
http://www.pharmacist.com/sites/default/files/JCPP_Pharmacists_Patient_Care_Process.pdf

effectiveness of treatment by monitoring clinical endpoints such as laboratory values and patient-reported outcomes, recommend dosing adjustments to tailor clinical response, access the safety profile of medications and evaluate patient risk for adverse outcomes, monitor and evaluate patient adherence and counsel patients on appropriate use and understanding of their treatments. One such activity of CMM routinely performed by pharmacists is medication therapy management (MTM). MTM consults are now required by the CMS Part D Prescription Drug Program and are particularly valuable at points when patients are transitioning between settings of care, when the risk of lost information and gaps in care is increased. Despite the known value of MTM services, technological barriers to information exchange limit the ability of MTM documents and associated recommendations to be shared with ease between settings of care.[141]

---

[141] ASHP-APhA Medication Management in Care Transitions Best Practices. Feb 2013

Appendix G: Glossary

Access Control Services (ACS)
Access Control service provides the mechanism for security authorizations that control the enforcement of security policies including: role-based access control, entity based access control, context based access control and the execution of consent directives.
http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=12&PrefixNumeric=108

Accountable Care Organizations (ACO)
Groups of doctors, hospitals and other health care providers, who come together voluntarily to give clinically coordinated care to their patients, often using payment forms other than fee-for-service.
https://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/ACO/index.html?redirect=/aco/

Accredited Standards Committee (ASC) X12
Develops and maintains electronic data interchange standards for global business markets, including standards for health care, insurance, transportation, finance, government, supply chain and other industries.
http://www.x12.org/

Admit/Discharge/Transfer (ADT) messages
Admission, Discharge and Transfer (ADT) messages are used to communicate episode details. ADT messages carry patient demographic information for HL7 communications, but also provide important information about trigger events (such as patient admit, discharge, transfer, registration, etc.). ADT messages are extremely common in HL7 processing and are among the most widely used of all message types.
http://www.gillogley.com/hl7_glossary.shtml
http://www.corepointhealth.com/resource-center/hl7-resources/hl7-adt

Agency for Healthcare Research and Quality (AHRQ)
The Nation's lead Federal agency for research on health care quality, costs, outcomes and patient safety. The AHRQ's mission is to produce evidence to make health care safer, higher quality, more accessible, equitable and affordable and to work within the U.S. Department of Health and Human Services and with other partners to make sure that the evidence is understood and used.
http://www.ahrq.gov/cpi/about/

American Health Information Community (AHIC)
The American Health Information Community was a federally chartered advisory committee that was formed in 2005-2008 to make recommendations to the Secretary of the U.S. Department of Health and Human Services on how to accelerate the development and adoption of health information technology.
http://www.phdsc.org/health_info/american-health-info.asp

API

An acronym standing for "Application Program Interface," an API is a software application function that can be invoked or controlled through interactions with other software applications. APIs allow the user experience to be seamless between two or more software applications since the APIs are working behind the actual user interface. For the purpose of the Roadmap the term is further defined as being specific API's that are in wide use and universally supported for particular functions across multiple vendors' products. They are published and accessible in a way that makes them easy for interested developers to find and use without a program host system intervention and for which there are no fees or other intellectual property restrictions that limit their availability to any competent and interested programmer. *Note: for this interoperability roadmap, the term is used as defined in this glossary.*

Architecture

The term "Architecture" is used in this report to refer to the collective components of a software system that interact in specified ways and across specified interfaces to ensure specified functionality. http://healthit.gov/sites/default/files/ptp13-700hhs_white.pdf

Authentication

Authentication and access control measures should ensure appropriate access to information and information processing facilities – including mainframes, servers, desktop and laptop clients, mobile devices, applications, operating systems and network services – and prevent inappropriate access to such resources.
http://it.med.miami.edu/x2232.xml

Authorization

Authorization represents the amount or type of information a person or system is allowed to access. For example, the absence of any authorization means a person or system may not access any information. Authorization to access all information means a person or system may access 100% of the information in the system. Authorization to access information regulated by 42 U.S.C. § 290dd-2means that information about that patient's substance abuse treatment could be released to the particular person who has been authorized to receive it. *Note: in other and prior health care contexts the term "authorization" may have been used in other ways, but for this interoperability roadmap, the term is used as defined in this glossary.*

"Basic" Choices

Basic Choice is the ability of an electronic health information system to capture, adjudicate, comply with and persist in downstream processing of the data an individual's documented choice about whether data about them should be available for electronic exchange within the learning health system. *Note: for this interoperability roadmap, the term is used as defined in this glossary.*

Blue Button Initiative

Blue Button is a tool to make patient medical records easily available for patients to download and share with members of their health care team. It allows individuals to create a single electronic file that can include all of their available personal health information.

http://www.va.gov/bluebutton/

http://bluebuttonconnector.healthit.gov/

Business Associate Agreement (BAA)

A contract between a covered entity and its business associate or a business associate and its subcontractor that must contain the elements specified at 45 CFR 164.504(e). For example, the contract must: Describe the permitted and required uses of protected health information by the business associate; Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law; and Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract

Care Connectivity Consortium

Founded in April 2011, the CCC is a consortium of health care providers working to improve and advance the technology available for comprehensive, secure, reliable and innovative electronic health information exchange across the country. Founded by five organizations – Geisinger Health System, Kaiser Permanente, Mayo Clinic, Intermountain Healthcare and Group Health Cooperative — its missions are to: develop solutions that enhance the capabilities of current technologies; allow more secure, reliable and effective sharing of data among disparate health record systems; offer these solutions to the broader HIE community; and accelerate the adoption of national HIE standards.

http://www.careconnectivity.org/about/details/

Centers for Disease Control and Prevention (CDC)

The Centers for Disease Control and Prevention (CDC), an agency within the U.S. Department of Health and Human Services, is the primary Federal agency for conducting and supporting public health activities in the United States. CDC's mission is to collaborate to create the expertise, information and tools that people and communities need to protect their health – through health promotion, prevention of disease, injury and disability and preparedness for new health threats.

http://healthfinder.gov/FindServices/Organizations/Organization.aspx?code=HR0039

http://www.cdc.gov

Centers for Medicare and Medicaid Services (CMS)

An agency within the US Department of Health & Human Services responsible for administration of several key federal health care programs. In addition to Medicare (the federal health insurance program for seniors) and Medicaid (the federal needs-based program), CMS oversees the Children's Health Insurance Program (CHIP) provisions in the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations that pertain to national standards for electronic health care

transactions and national identifiers for providers, health plans and employers, and the Clinical Laboratory Improvement Amendments (CLIA), among other services.
http://searchhealthit.techtarget.com/definition/Centers-for-Medicare-Medicaid-Services-CMS
http://www.cms.gov

Certification Commission for Health Information Technology (CCHIT)
The Certification Commission for Health Information Technology (CCHIT) was a private, nonprofit initiative to accelerate the adoption of health information technology by creating an efficient, credible and sustainable certification program for electronic health records and their networks. It ceased operations in November 2014.
http://www.phdsc.org/standards/certification-commission.asp

Certified EHR Technology (CEHRT)
Certified EHR technology gives assurance to purchasers and other users that an EHR system or module offers the necessary technological capability, functionality and security to help them meet the meaningful use criteria.
http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Certification.html

Clinical Decision Support (CDS)
Clinical decision support (CDS) provides clinicians, staff, patients or other individuals with knowledge and person-specific information, intelligently filtered or presented at appropriate times, to enhance health and health care. CDS encompasses a variety of tools to enhance decision-making in the clinical workflow. These tools include computerized alerts and reminders to care providers and patients; clinical guidelines; condition-specific order sets; focused patient data reports and summaries; documentation templates; and diagnostic support and contextually relevant reference information, among other tools.
http://www.healthit.gov/policy-researchers-implementers/clinical-decision-support-cds

Clinical Quality Measurement (CQM)
Clinical quality measures, or CQMs, are tools that help measure and track the quality of health care services provided by eligible professionals, eligible hospitals and critical access hospitals (CAHs) within our health care system. These measures use data associated with providers' ability to deliver high-quality care or relate to long term goals for quality health care.
http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/ClinicalQualityMeasures.html

CMS EHR Incentive Programs
The Medicare and Medicaid Electronic Health Care Record (EHR) Incentive Programs provide incentive payments to eligible professionals, eligible hospitals and critical access hospitals (CAHs) as they adopt, implement, upgrade or demonstrate meaningful use of certified EHR technology.
http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms/

Common Data Element (CDE)
Clinical concepts that contain standardized and structured metadata, have unambiguous intent and a clearly delineated value domain. These CDEs, such as "systolic blood pressure," would define a curated, universal specification for each clinical or administrative concept, optimizing the data to be reused across the QI ecosystem.
http://www.healthit.gov/sites/default/files/HITEnabledQualityImprovement-111214.pdf

Comprehensive Medication Management (CMM)
The standard of care that ensures that a patient's medications are appropriate, effective, safe and taken as intended.
http://cpnp.org/resource/mhc/2013/10/comprehensive-medication-management-patients-mental-illnesses

Computerized Physician Order Entry (CPOE)
Computerized Physician Order Entry (or CPOE) is the process of capturing a physician's instructions for a patient's care electronically to improve the efficiency of care delivery.
http://www.healthcareitnews.com/directory/computerized-physician-order-entry-cpoe

Consent
Agreement to an action based on knowledge of what the action involves and its likely consequences.
http://medical-dictionary.thefreedictionary.com/consent

Consolidated-Clinical Data Architecture (C-CDA)
The HL7 "consolidated" clinical document architecture (C-CDA) standard contains a library of CDA template standards and represents a single, unified implementation guide for multiple electronic clinical documents.
http://www.practicefusion.com/blog/understanding-c-cda-standard-ehr-certification-meaningful-use/

Consumer Data Privacy in a Network World
A framework for protecting privacy and promoting innovation in the global digital economy.
http://repository.cmu.edu/jpc/vol4/iss2/5/

CPT
The Current Procedural Terminology (CPT) code set is a medical code set maintained by the American Medical Association through the CPT Editorial Panel. The CPT coding system offers doctors across the country a uniform process for coding medical services that streamlines reporting and increases accuracy and efficiency.
http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/cpt/cpt-process-faq/code-becomes-cpt.page

CVX

CVX codes are provided for each available vaccine used in the United States. When an MVX (manufacturer) code is paired with a CVX (vaccine administered) code, the specific trade named vaccine may be indicated.

http://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=cvx

Data Access Framework (DAF)

A Standards & Interoperability (S&I) Framework initiative to define the standards and framework necessary for clinicians, providers and healthcare professionals to gain access to patient data within their own organization and from external organizations that may contain patient data.

http://wiki.siframework.org/Data+Access+Framework+Homepage

Data Provenance

Data provenance refers to the process of tracing and recording the origins of data and its movement between databases and is central to the validation of data. There is a Standards and Interoperability (S&I) Framework initiative working to define standards that support data provenance.

http://db.cis.upenn.edu/DL/fsttcs.pdf

http://wiki.siframework.org/Data+Provenance+Initiative

Data Segmentation for Privacy (DS4P)

The term "data segmentation" refers to the process of sequestering certain data elements from capture, access or view that are perceived by a legal entity, institution, organization, or individual as being undesirable to share. This basic definition, however, does not account for the multiple permutations of segmentation in the health care context (i.e., granularity), nor does it adequately capture the varied considerations required for development of segmentation policy. There is a Standards and Interoperability (S&I) Framework initiative working to define standards that support DS4P.

http://wiki.siframework.org/Data+Segmentation+for+Privacy+Charter+and+Members

Data Use and Reciprocal Support Agreement (DURSA)

The Data Use and Reciprocal Support Agreement (DURSA) is a comprehensive, multi-party trust agreement that was signed by all Nationwide Health Information Network participants, both public and private, wishing to participate in the NwHIN Exchange, now referred to as the eHealth Exchange. The DURSA provides the legal framework governing participation in the eHealth Exchange by requiring the signatories to abide by a common set of terms and conditions.

http://www.healthit.gov/sites/default/files/draft_nhin_trial_implementations_production_dursa-3.pdf

http://www.healthewayinc.org/images/Content/Documents/Application-Package/restatement_i_of_the_dursa_9.30.14_final.pdf

Deterministic Matching Algorithm

Deterministic Matching uses sets of predetermined rules to guide the matching process. The rules rely on a series of exact matches between data elements to identify when records match. It is most successful when the data is of relatively high quality or is dominated by reliable unique identifiers for

records. Deterministic matching is less successful when the data is incomplete or inaccurate, when there are many spelling or transcription errors, or lots of inconsistencies (e.g., frequent name changes).
https://www.hln.com/assets/pdf/mpi_generic_final.pdf

Digital Imaging and Communications in Medicine (DICOM)
DICOM is an application layer network protocol for the transmission of medical images, waveforms and accompanying information.
http://whatis.techtarget.com/definition/DICOM-Digital-Imaging-and-Communications-in-Medicine

Direct Protocol
Direct uses established standards and protocols to enable secure health information exchange through a simple, scalable approach. Direct allows authorized users to send authenticated, encrypted health information directly to known recipients via the Internet. Direct offers a means of transmitting health information in support of core Stage 2 meaningful use measures including the communication of summary care records, referrals, discharge summaries and other clinical documents.
http://www.healthit.gov/policy-researchers-implementers/direct-project
http://wiki.directproject.org/

Directed Exchange (push)
Organizations need to send information to one another, often in an unsolicited manner (i.e., , without the recipient specifically asking for the information). The Direct protocol was developed by the S&I Framework and utilizes email standards, but in a secure manner, with the primary protocol utilizing secure mail transport (SMTP). Direct supports a secure e-mail transaction that is appropriate for many different uses, including provider-to-provider, provider-to-consumer, provider-to-payer and many other types of transactions. The Direct protocol is an all-purpose protocol; it does not care what type of information is transported. To be used effectively, however, a trust relationship must exist between participants to ensure that a message reaches the intended party and not someone else. Other technologies have also been in use for some time to support unsolicited transmission of information including, secure File Transfer Protocol (sFTP) and Simple Object Access protocol [SOAP] and Representational State Transfer (REST).
http://www.healthit.gov/policy-researchers-implementers/direct-project
http://wiki.directproject.org/

DirectTrust
DirectTrust is an independent, non-profit trade association created by and for participants in the Direct community. It has established a set of technical, legal and business standards, expressed as policy and best practice recommendations, which members of the trust community agree to follow, uphold and enforce. DirectTrust offers an accreditation program that assesses organizations' adherence to these standards.
http://www.directtrust.org/

eHealth Exchange
The eHealth Exchange, formerly known as the NwHIN Exchange, is a group of federal agencies and non-federal organizations that came together under a common mission and purpose to improve patient care, streamline disability benefit claims and improve public health reporting through secure, trusted and interoperable health information exchange.
http://healthewayinc.org/index.php/exchange

EHR|HIE Interoperability Workgroup (IWG)
The EHR|HIE Interoperability Workgroup (IWG) is a New York eHealth Collaborative-led coalition of 19 States (representing 52% of the U.S. population), 20 electronic health record (EHR) vendors and 22 health information exchange (HIE) vendors. The workgroup was launched in February 2011 to leverage existing standards and develop consistent implementation guides to support interoperability between HIE software platforms and the applications that interface with them.
http://nyehealth.org/news-list/onc-awards-the-ehrhie-interoperability-workgroup-exemplar-hie-governance-program-cooperative-agreement/

Electronic Health Record (EHR)
An electronic health record (EHR) is a digital version of a patient's paper chart. EHRs are real-time, patient-centered records that make information available instantly and securely to authorized users. While an EHR does contain the medical and treatment histories of patients, an EHR system is built to go beyond standard clinical data collected in a provider's office and can be inclusive of a broader view of a patient's care.
http://www.healthit.gov/providers-professionals/faqs/what-electronic-health-record-ehr

Electronic Healthcare Network Accreditation Commission (EHNAC)
Founded in 1993, the Electronic Healthcare Network Accreditation Commission (EHNAC) is an independent, federally recognized standards development organization and tax-exempt, 501(c)(6) non-profit accrediting body designed to improve transactional quality, operational efficiency and data security in healthcare.
https://www.ehnac.org/about/

Encryption/decryption
Encryption is the process of encoding messages or information in such a way that only authorized parties can read it.
http://en.wikipedia.org/wiki/Encryption

eXtensible Markup Language (XML)
Extensible Markup Language (XML) is a simple, very flexible text format derived from SGML (ISO 8879). Originally designed to meet the challenges of large-scale electronic publishing, XML is also playing an increasingly important role in the exchange of a wide variety of data on the Web and elsewhere.
http://www.w3.org/XML/

Fair Information Practices Principles (FIPPs)

FIPPs are the widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy.
http://www.nist.gov/nstic/NSTIC-FIPPs.pdf

Fast Healthcare Interoperability Resources (FHIR)

Fast Healthcare Interoperability Resources (FHIR, pronounced "Fire") defines a set of "Resources" that represent granular clinical concepts. The resources can be managed in isolation, or aggregated into complex documents. Technically, FHIR is designed for the web; the resources are based on simple XML or JSON structures, with an http-based RESTful protocol where each resource has predictable URL. Where possible, open internet standards are used for data representation.
http://wiki.hl7.org/index.php?title=FHIR

Federal Health Architecture (FHA)

The Federal Health Architecture (FHA) is an e-government initiative managed by the Office of the National Coordinator for Health IT (ONC) within the Department of Health and Human Services (HHS). FHA was formed to coordinate health IT activities among the more than 20 federal agencies that provide health and healthcare services to citizens.
http://www.healthit.gov/sites/default/files/pdf/fact-sheets/federal-health-architecture.pdf

Granular Choice

The ability of an electronic health record system to capture, adjudicate, comply with and persist in the subsequent uses of the data per an individual's documented choice. Granular choice starts with distinctions between legally sensitive clinical conditions, such as mental health or HIV/AIDS status and evolves over time to enable choice about disclosure to specifically identified participants in the healthcare system. *Note: for this interoperability roadmap, the term is used as defined in this glossary.*

Health Information Exchange (HIE)

Electronic health information exchange (HIE) allows doctors, nurses, pharmacists, other health care providers and patients to appropriately access and securely share a patient's vital medical information electronically—improving the speed, quality, safety and cost of patient care.
http://www.healthit.gov/providers-professionals/health-information-exchange/what-hie

Health Information Organization (HIO)

A Health information organization (HIO) is a multi-stakeholder organization created to facilitate health information exchange among stakeholders of that region's healthcare system.
http://en.wikipedia.org/wiki/Regional_Health_Information_Organization

Health Information Service Provider (HISP)

The term Health Information Service Provider (HISP) has been used by the Direct project both to describe a function (the management of security and transport for directed exchange) and an organizational model (an organization that performs HISP functions on behalf of the sending or receiving

organization or individual). In this best practice document, we are mainly concerned with the HISP organization and the implications for privacy, security and transparency when the HISP is a separate business entity from the sending or receiving organization.
http://wiki.directproject.org/Best+Practices+for+HISPs

Health Information Technology for Economic and Clinical Health (HITECH) Act
The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 provides HHS with the authority to establish programs to improve health care quality, safety and efficiency through the promotion of health IT, including electronic health records and private and secure electronic health information exchange. Learn more about select portions of the HITECH Act that relate to ONC's work.
http://www.healthit.gov/policy-researchers-implementers/health-it-legislation

Health Information Technology Policy Committee (HITPC)
The American Recovery and Reinvestment Act (ARRA) requires the Comptroller General of the United States to appoint thirteen of twenty members to the HIT Policy Committee, a body which makes recommendations on creating a policy framework for the development and adoption of a nationwide health information technology infrastructure, including standards for the exchange of patient medical information.
http://www.gao.gov/about/hcac/hitpc.html

Health Information Technology Standards Committee (HITSC)
The Health Information Technology (HIT) Standards Committee is a federal advisory committee (FACA) charged with making recommendations to the Office of the National Coordinator for Health Information Technology (ONC) on standards, implementation specifications and certification criteria for the electronic exchange and use of health information.
http://www.phdsc.org/standards/health-information/HITSC.asp

Health Insurance Portability and Accountability Act (HIPAA)
HIPAA is the acronym of the Health Insurance Portability and Accountability Act of 1996. The Office for Civil Rights (OCR) enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; the HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.
http://www.hhs.gov/ocr/privacy/

Health IT Certification Program
The Office of the National Coordinator for Health Information Technology (ONC) Certification Program helps to ensure that Electronic Health Record (EHR) technologies meet the standards and certification criteria adopted by the Secretary of Health and Human Services to allow providers and hospitals achieve meaningful use and participate in the CMS EHR Incentive Programs.
http://www.healthit.gov/policy-researchers-implementers/about-onc-hit-certification-program

Health Level Seven (HL7)
Founded in 1987, Health Level Seven International (HL7) is a not-for-profit, ANSI-accredited standards developing organization. HL7 develops and maintains a framework and related standards for the exchange, integration, sharing and retrieval of electronic health information, defining how information is packaged and communicated from one party to another and setting the language, structure and data types required for seamless integration between systems.
http://www.hl7.org/about/index.cfm?ref=nav

Health Quality Domain Analysis Model (QI DAM)
This document seeks to define the common concepts and semantics involved in modeling reasoning within the various aspects of the health quality domain, with the goal of providing a common conceptual foundation that other specifications can use whenever the need to express and communicate expression logic arises.
http://www.hl7.org/implement/standards/product_brief.cfm?product_id=359

Healthcare Provider Directory (HPD)
The IHE Healthcare Provider Directory (HPD) profile supports management of healthcare provider information including public information on people and organizations across enterprises in a directory structure. HPD directory structure is a listing of healthcare providers that are classified by provider type, specialties, credentials, demographics and service locations.
http://wiki.ihe.net/index.php?title=Healthcare_Provider_Directory

ICD-9-CM/ICD-10-CM/PCS
ICD-9-CM and ICD-10-CM/PCS are forms of medical coding. ICD-10-CM/PCS will enhance accurate payment for services rendered and facilitate evaluation of medical processes and outcomes. The new classification system provides significant improvements through greater detailed information and the ability to expand in order to capture additional advancements in clinical medicine. The International Classification of Diseases (ICD) is maintained by the World Health Organization and is the most widely used disease classification system in the world. In the U.S., the National Center for Health Statistics (NCHS) adapted ICD-9 CM for diagnosis and procedure codes. NCHS and CMS are responsible for maintaining and distributing ICD-9 CM. The U.S. is moving towards ICD-10 CM, with a required implementation date of October 1, 2015.
https://www.uth.edu/dotAsset/2409977.pdf

IEEE
The Institute of Electrical and Electronic Engineers (IEEE) is a global association and organization of professionals working toward the development, implementation and maintenance of technology-centered products and services. IEEE is a nonprofit organization founded in 1963. It works solely toward innovating, educating and standardizing the electrical and electronic development industry. It is best known for its development of standards such as IEEE 802.11.
http://www.ieee.org/education_careers/education/standards/standards_glossary.html

Innovation Community

The innovation community is comprised of entrepreneurs, startups and developers that build new Health IT technology and bring it to market; the early adopters who implement and test emerging technology; and the venture capital firms and incubators/accelerators that invest in Health IT and nurture early stage companies to success and the scientists who are evaluating new Health IT solutions and using Health IT to conduct clinical research. *Note: for this interoperability roadmap, the term is used as defined in this glossary.*

Integrating the Healthcare Enterprise (IHE)

IHE is an initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information. IHE promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical needs, through the development of architectures and profiles to meet specific use case needs.

http://www.ihe.net/

International Health Terminology Standards Development Organisation (IHTSDO)

Determines global standards for health terminology, most notably for SNOMED CT (Systematized Nomenclature of Medicine--Clinical Terms).

International Telecommunications Union Telecommunication Standardization Sector (ITU-T)

Develops international standards and recommendations defining elements in the global infrastructure of information and communication technologies; most notably within health the standard for X.509 digital certificates.

Internet Engineering Task Force (IETF)

Producing technical documents and standards to guide design, use and management of nearly all interactions on the Internet, including the most basic Internet protocols.

Interoperability

In the context of this Roadmap, interoperability is defined as the ability of a system to **exchange** electronic health information with and **use** electronic health information from other systems without special effort on the part of the user. Interoperability is made possible by the implementation of standards.

http://www.ieee.org/education_careers/education/standards/standards_glossary.html

JASON

JASON is an independent group of scientists that advises the Federal government on matters of science and technology.

http://www.healthit.gov/buzz-blog/from-the-onc-desk/robust-health-data-infrastructure/
http://healthit.gov/sites/default/files/2014-JASON-data-for-individual-health.pdf

Learning Health System (LHS)
The concept of a continuously Learning Health System (LHS), first expressed by the Institute of Medicine in 2007, is now being rapidly adopted across the country and around the world. The LHS is based on cycles that include data and analytics to generate knowledge, leading feedback of that knowledge to stakeholders, with the goal to change behavior to improve health and to transform organizational practice.
http://healthinformatics.umich.edu/lhs

Level of Assurance (LOA)
Authentication focuses on verifying a person's identity based on the reliability of a credential offered. LOA refers to how much confidence a relying party has that the credential presented is in the possession of the person whose identity is being asserted. The Office of Management and Budget (OMB 04-04) describes four levels of identity authentication assurance levels, with Level 1 being the lowest level of assurance and Level 4 being the highest level of assurance.
https://www.cio.wisc.edu/security-initiatives-levels.aspx

Lightweight Directory Access Protocol (LDAP)
LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet.
http://searchmobilecomputing.techtarget.com/definition/LDAP

Logical Observation Identifiers Names and Codes (LOINC)
LOINC, the Logical Observation Identifiers Names and Codes, is a universal code system for tests, measurements and observations. LOINC started in 1994 by the Regenstrief Institute. LOINC is the standardization of laboratory and other clinical observation values, so that systems can communicate electronically without having to map data elements. Historically, each laboratory, health system and vendor has recorded laboratory values (such as an HA1C result) with their own proprietary vocabulary or internal code values. Consequently, laboratories and systems could send and receive laboratory results electronically, but only with a significant amount of work to map the values and with no guarantee that the values were interpreted and mapped correctly. NLM has provided partial support for the ongoing production and free dissemination of LOINC since 1999.
http://loinc.org/

Long-Term Post-Acute Care (LTPAC)
LTPAC Settings (e.g., Skilled Nursing Facility (SNF), Home Health, Inpatient Rehab, Long Term Acute Care Hospital, Hospice). This category of providers serves some of the nation's most vulnerable individuals and uses a significant portion of the Medicare and Medicaid budgets. Patients served by these providers experience frequent transitions in care and episodes of care coordination with eligible hospitals and professionals. Some of these providers may need interoperable EHR technology to support new care delivery and payment models in the Affordable Care Act and in private sector initiatives.
http://aspe.hhs.gov/daltcp/reports/2013/EHRPIap.shtml#appendE
http://aspe.hhs.gov/daltcp/reports/2013/ehrpi.shtml#ineligible

Long-Term Services & Supports (LTSS)
Assistance with activities of daily living and instrumental activities of daily living provided to older people and adults with disabilities that cannot perform these activities on their own due to a physical, cognitive, or chronic health conditions. LTSS may provide care, case management and service coordination to people who live in their own home, a residential setting, a nursing facility, or other institutional setting. LTSS also include supports provided to family members and other unpaid caregivers. LTSS may be provided in institutional and community settings.
http://www.acl.gov/Programs/CDAP/OIP/docs/2402-a-Guidance.pdf

Meaningful Use
Meaningful Use describes the use of certified electronic health record technology (cEHRt) to improve quality, safety, efficiency and reduce health disparities; engage patients and family; improve care coordination and population and public health.
http://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives

Medicaid Delivery System Reform Incentive Payment (DSRIP)
"Delivery System Reform Incentive Payment" or DSRIP programs are another piece of the dynamic and evolving Medicaid delivery system reform landscape. DSRIP initiatives are part of broader Section 1115 Waiver programs and provide states with significant funding that can be used to support hospitals and other providers in changing how they provide care to Medicaid beneficiaries.
http://kff.org/medicaid/issue-brief/an-overview-of-delivery-system-reform-incentive-payment-waivers/

Medication Therapy Management (MTM)
Medication therapy management is a service or group of services that optimize therapeutic outcomes for individual patients. Medication therapy management services include medication therapy reviews, pharmacotherapy consults, anticoagulation management, immunizations, health and wellness programs and many other clinical services. Pharmacists provide medication therapy management to help patients get the best benefits from their medications by actively managing drug therapy and by identifying, preventing and resolving medication-related problems.
http://www.pharmacist.com/mtm

National Center for Health Statistics (NCHS)
The National Vital Statistics System is the oldest and most successful example of inter-governmental data sharing in public health and the shared relationships, standards and procedures form the mechanism by which NCHS collects and disseminates the nation's official vital statistics.
http://www.cdc.gov/nchs/nvss.htm

National Council for Prescription Drug Plans (NCPDP)
The National Council for Prescription Drug Programs (NCPDP) is an American National Standards Institute (ANSI)-accredited Standards Development Organization. The purpose of The NCPDP Guide is to provide parameters for utilizing an ANSI approved health care ID card standard that clearly and consistently defines the information and format required by the pharmacy provider.
http://www.ncpdp.org/NCPDP/media/pdf/NCPDPpharmacyIdCardFactSheet.pdf

National Council for Prescription Drug Programs (NCPDP) SCRIPT
The National Council for Prescription Drug Programs SCRIPT Standard is used to transmit electronic prescriptions from a physician or prescriber to the pharmacy; specific messages include New, Change, Renewal, Cancellation and Fill Status.
http://healthit.ahrq.gov/key-topics/ncpdp

National Drug Code (NDC)
The NDC, or National Drug Code, is a unique 10-digit, 3-segment number. It is a universal product identifier for human drugs in the United States. The code is present on all non-prescription (OTC) and prescription medication packages and inserts in the US.
http://www.drugs.com/ndc.html

National eHealth Collaborative (NeHC)
National eHealth Collaborative is a public-private partnership that aims to enable secure and interoperable nationwide health information exchange through education and stakeholder engagement. In December 2013 NeHC was absorbed by the HIMSS Foundation.
http://www.healthcareitnews.com/directory/national-ehealth-collaborative-nehc

National Information Exchange Model (NIEM)
NIEM—the National Information Exchange Model—is a community-driven, standards-based approach to exchanging information. NIEM brings together diverse communities that collectively leverage tools, processes and technologies to increase efficiencies and improve decision-making.
https://www.niem.gov/aboutniem/Pages/niem.aspx

National Institute of Standards and Technology (NIST)
Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life.
http://www.nist.gov/public_affairs/general_information.cfm

National Library of Medicine (NLM)
The National Library of Medicine (NLM), on the campus of the National Institutes of Health in Bethesda, Maryland, has been a center of information innovation since its founding in 1836. The world's largest biomedical library, NLM maintains and makes available a vast print collection and produces electronic

information resources on a wide range of topics that are searched billions of times each year by millions of people around the globe. It manages the world's largest medical library and is part of the National Institutes of Health (NIH) that also manages and makes health terminology standards available such as the normalized drug vocabulary, RxNorm, NDF-RT and US Edition SNOMED-CT.
http://www.nlm.nih.gov/about/

National Plan & Provider Enumeration System (NPPES)
The Centers for Medicare & Medicaid Services (CMS) has developed the National Plan and Provider Enumeration System (NPPES) to assign unique identifiers to health care providers. The National Provider Identifier (NPI) has been the standard identifier for health care providers since May 2007.
http://www.nber.org/data/npi.html

National Provider Identifier (NPI)
The National Provider Identifier (NPI) is a Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Standard. The NPI is a unique identification number for covered health care providers. Covered health care providers and all health plans and health care clearinghouses must use the NPIs in the administrative and financial transactions adopted under HIPAA. The NPI is a 10-position, intelligence-free numeric identifier (10-digit number).
https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/NationalProvIdentStand/index.html?redirect=/NationalProvIdentStand/

National Strategy for Trusted Identities in Cyberspace (NSTIC)
The National Strategy for Trusted Identities in Cyberspace (NSTIC, or Strategy) is a White House initiative to work collaboratively with the private sector, advocacy groups, public sector agencies and other organizations to improve the privacy, security and convenience of online transactions.
http://www.nist.gov/nstic/about-nstic.html

National Study of Long-Term Care Providers (NSLTCP)
The biennial National Study of Long-Term Care Providers (NSLTCP), sponsored by the U.S. Centers for Disease Control and Prevention's National Center for Health Statistics (NCHS), is a groundbreaking initiative to monitor trends in the major sectors of paid, regulated long-term care services providers.
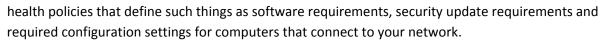http://www.cdc.gov/nchs/data/nsltcp/NSLTCP_FS.pdf

Nationwide Health Information Network (NwHIN)
The Nationwide Health Information Network is a set of standards, services and policies that enable the secure exchange of health information over the Internet.
http://www.healthit.gov/policy-researchers-implementers/nationwide-health-information-network-nwhin

Network Access Protection (NAP)
Network Access Protection (NAP) is a client health policy creation, enforcement and remediation technology that is included in Windows Vista® and Windows Server® 2008. With NAP, you can establish

health policies that define such things as software requirements, security update requirements and required configuration settings for computers that connect to your network.
http://technet.microsoft.com/en-us/library/cc754378%28v=ws.10%29.aspx

OAUTH2

OAuth 2 is an authorization framework that enables applications to obtain limited access to user accounts on an HTTP service. It works by delegating user authentication to the service that hosts the user account and authorizing third-party applications to access the user account. OAuth 2 provides authorization flows for web and desktop applications and mobile devices.
https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2

Office for Civil Rights (OCR)

The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; the HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.
http://www.hhs.gov/ocr/office/about/index.html

Office of Consumer eHealth (OCeH)

OCEH works to empower patients and caregivers to be partners in their health care through the adoption and use of health IT.
http://www.ilhitrec.org/ilhitrec/pdf/ONCSummaryCongress_July2013.pdf

Office of the Assistant Secretary for Preparedness and Response (ASPR)

The Office of the Assistant Secretary for Preparedness and Response was created under the Pandemic and All Hazards Preparedness Act in the wake of Katrina to lead the nation in preventing, preparing for and responding to the adverse health effects of public health emergencies and disasters. ASPR focuses on preparedness planning and response, building federal emergency medical operational capabilities, countermeasures research, advance development and procurement, and providing grants to strengthen the capabilities of hospitals and health care systems in public health emergencies and medical disasters.
http://www.phe.gov/about/aspr/pages/default.aspx

Office of the National Coordinator for Health Information Technology (ONC)

The Office of the National Coordinator for Health Information Technology (ONC) is at the forefront of the administration's health IT efforts and is a resource to the entire health system to support the adoption of health information technology and the promotion of nationwide health information exchange to improve health care. ONC is organizationally located within the Office of the Secretary for the U.S. Department of Health and Human Services (HHS).
http://www.healthit.gov/newsroom/about-onc

OpenID Connect
OpenID, which was first created in 2005, allows web sites and authentication services to exchange security information in a standardized way. The goal of OpenID Connect is to allow an end user to log in once and access multiple, disparate resources on and off the Web. The specification, which has the backing of numerous cloud providers, including Google and Microsoft, is expected to pave the way for companies to replace their on-premise identity and access management (IAM) systems with cloud offerings.
http://whatis.techtarget.com/definition/OpenID

Organization for the Advancement of Structured Information Standards (OASIS)
OASIS is a non-profit consortium that drives the development, convergence and adoption of open standards for the global information society, including many XML-based specifications and the specification for SOAP web services. OASIS promotes industry consensus and produces worldwide standards for security, Internet of Things, cloud computing, energy, content technologies, emergency management and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets and protect the right of free choice of technology.
https://www.oasis-open.org/org

Persist or Persistence
The idea that a particular data element stays with the data as it flows downstream and is reprocessed and reused the permissions that may limit access to, use of, or disclosure of an individual's data must persist in the data to ensure proper privacy compliance. *Note: for this interoperability roadmap, the term is used as defined in this glossary.*

Personal Health Record (PHR)
A personal health record (PHR) is an electronic application used by patients to maintain and manage their health information in a private, secure and confidential environment.
http://www.healthit.gov/providers-professionals/faqs/what-personal-health-record

Person-Centered
ONC's vision for a person-centered learning health system: the power of each individual is developed and unleashed to be active in managing their health and partnering in their health care, enabled by information and technology. Health care is a partnership between the patient, their caregivers, the care team and supporting services.
http://www.healthit.gov/policy-researchers-implementers/person-center

Policy Decision Point (PDP)
The point where policy decisions are made. In the case of NAP, this is the NAP health policy server.
http://msdn.microsoft.com/en-us/library/ee380787.aspx

Policy Enforcement Point (PEP)
The point where the policy decisions are actually enforced.
http://msdn.microsoft.com/en-us/library/ee380787.aspx

Population Health
Population health is defined as the health outcomes of a group of individuals, including the distribution of such outcomes within the group.
http://www.improvingpopulationhealth.org/blog/what-is-population-health.html

Prescription Drug Monitoring Programs (PDMP)
Prescription drug monitoring programs (PDMPs) maintain statewide electronic databases of prescriptions dispensed for controlled substances (i.e., prescription drugs of abuse that are subject to stricter government regulation).
http://www.fas.org/sgp/crs/misc/R42593.pdf

President's Council of Advisors on Science and Technology (PCAST)
PCAST is an advisory group of the nation's leading scientists and engineers who directly advise the President and the Executive Office of the President. PCAST makes policy recommendations in the many areas where understanding of science, technology and innovation is key to strengthening our economy and forming policy that works for the American people.
http://www.whitehouse.gov/administration/eop/ostp/pcast/about

Probabilistic Matching Algorithm
Probabilistic Matching is a process whereby an estimate is made of the probability that two records are for the same person based on the degree to which certain fields in the two records match. Two thresholds are then set: All record pairs whose probability is above the higher threshold are considered to be matches; all record pairs whose probability is below the lower threshold are considered not to be matches. The disposition of record pairs whose probability falls in between the two thresholds is considered to be uncertain and they require additional review. An alternate method is Deterministic Matching Algorithm.
https://www.hln.com/assets/pdf/mpi_generic_final.pdf

Protected Health Information (PHI)
The HIPAA Privacy Rule defines PHI as individually identifiable health information, held or maintained by a covered entity or its business associates acting for the covered entity that is transmitted or maintained in any form or medium (including the individually identifiable health information of non-U.S. citizens).
http://privacyruleandresearch.nih.gov/pr_07.asp

Provider Enrollment, Chain and Ownership System (PECOS)
PECOS supports the Medicare Provider and Supplier enrollment process by allowing registered users to securely and electronically submit and manage Medicare enrollment information.
https://pecos.cms.hhs.gov/pecos/login.do

Public Health

Public health is the science of protecting and improving the health of families and communities through promotion of healthy lifestyles, research for disease and injury prevention and detection and control of infectious diseases. Overall, public health is concerned with protecting the health of entire populations. These populations can be as small as a local neighborhood, or as big as an entire country or region of the world.

http://www.cdcfoundation.org/content/what-public-health

Publish, Subscribe, Notification

Services allow participants to know if information is available for them to take action as they see fit, rather than having all of the information sent directly to them. Notification services can also support more automated processes that might rely on this information to feed other workflows or processes. Today, notification is handled in a variety of ways supported by a variety of technologies, including use of HL7 v2 Admit/Discharge/Transfer (ADT) messages passed between organizations and the Blue Button Toolkit, which includes the ability to subscribe to a resource and be notified as new information is available. *Note: for this interoperability roadmap, the term is used as defined in this glossary.*

Public Key Infrastructure (PKI)

A set of hardware, software, people, policies and procedures needed to create, manage, distribute, use, store and revoke digital certificates... (which are) electronic document(s) used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

http://en.wikipedia.org/wiki/Public_key_infrastructure
http://en.wikipedia.org/wiki/Public_key_certificate

Quality Reporting Data Architecture (QRDA)

QRDA is a document format that provides a standard structure with which to report quality measure data to organizations that will analyze and interpret the data.

http://www.hl7.org/implement/standards/product_brief.cfm?product_id=35

Query (pull)

Organizations and individuals will need to perform secure searches for health data from known or unknown sources. Information query (and its associated response by the other party) is a complex activity. Queries must be structured in a way that the recipient can – in an automated way – not only understand what is being requested, but identify whether the information is present and disclosure is authorized in response. Query/response transactions must be encrypted for security. They must be permitted under the laws and policies of all relevant jurisdictions (federal, state and local). A variety of technologies and standards are in use to support query, including IHE profiles, which have become the basis for a variety of efforts (including the eHealth Exchange, EHR|HIE Work Group and the Care Connectivity Consortium). Web services are widely used with these and other standards to enable

query/response transactions. *Note: for this interoperability roadmap, the term is used as defined in this glossary.*

Reference Information Model (RIM)
"The RIM is a large, pictorial representation of the HL7 clinical data (domains) and identifies the life cycle that a message or groups of related messages will carry. It is a shared model between all domains and, as such, is the model from which all domains create their messages."
http://www.hl7.org/implement/standards/rim.cfm

Representational State Transfer (RESTful)
RESTful (Representational State Transfer) is an architectural style and an approach to communications that is often used in the development of Web services. The use of REST is often preferred over SOAP (Simple Object Access Protocol). The primary popularity of REST is that it is simpler to configure and deploy than SOAP.
http://searchsoa.techtarget.com/definition/REST

RESTful API
A method of allowing communication between a Web-based client and server that employs representational state transfer (REST) constraints. A RESTful API is an application program interface (API) that uses HTTP requests to GET, PUT, POST and DELETE data. RESTful APIs break down a transaction to create a series of small modules, each of which addresses a particular underlying part of the transaction.
http://searchcloudstorage.techtarget.com/definition/RESTful-API

Rules of the Road
The set of basic rules that will provide the needed underpinning to support electronic health information exchange nationwide. *Note: for this interoperability roadmap, the term is used as defined in this glossary.*

RxNorm
RxNorm provides normalized names for clinical drugs and links its names to many of the drug vocabularies commonly used in pharmacy management and drug interaction software. The NLM began development of RxNorm in 2001. RxNorm code sets are a way of representing medication data, such as the name, active ingredients, strength and dosage. RxNorm creates a normalized name for each medication, so that sending and receiving systems interpret the medication data in the same way. RxNorm names and codes for medications newly approved by FDA are issued weekly. The full RxNorm release is updated on a monthly basis.
http://www.nlm.nih.gov/research/umls/rxnorm/

Secure File Transport Protocol (SFTP)
SFTP uses the Secure Shell protocol (SSH) to transfer files. Unlike FTP, it encrypts both commands and data, preventing passwords and sensitive information from being transmitted openly over the network.
http://en.wikipedia.org/wiki/File_Transfer_Protocol#Secure_FTP

Secure/Multipurpose Internet Mail Extensions (S/MIME)
S/MIME is a standard used to encode binary files for transfer via SMTP-based e-mail.
http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

Security Assertion Markup Language (SAML)
SAML, (pronounced sam-el) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. SAML is a product of the OASIS Security Services Technical Committee.
http://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

Semantics
Terminology standards (or standardized nomenclature) define words permitting representatives of an industry or parties to a transaction to use a common, clearly understood language.
http://www.nist.gov/standardsgov/definestandards.cfm

Service/Service-oriented Architecture (SOA)
SOA is based on distinct pieces of software providing application functionality as services to other applications via a protocol. Depending on the service design approach taken, each SOA service is designed to perform one or more activities by implementing one or more service operations. As a result, each service is built as a discrete piece of code. This makes it possible to reuse the code in different ways throughout the application by changing only the way an individual service interoperates with other services that make up the application, versus making code changes to the service itself. SOA design principles are used during software development and integration.
http://en.wikipedia.org/wiki/Service-oriented_architecture

Simple Mail Transport Protocol (SMTP)
Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission. SMTP defines message transport, not the message content.
http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

Simple Object Access Protocol (SOAP)-based Web Services/Web Services Description Language (WSDL)
SOAP is a protocol specification for exchanging structured information in the implementation of web services in computer networks. A Web service is a method of communication between two electronic devices over a network. The Web Services Description Language (WSDL pronounced wiz'-dul) is an XML-based interface definition language that is used for describing the functionality offered by a web service.
http://en.wikipedia.org/wiki/SOAP
http://en.wikipedia.org/wiki/Web_service
http://en.wikipedia.org/wiki/Web_Services_Description_Language

Standard
Common and repeated use of rules, conditions, guidelines or characteristics for products or related processes and production methods and related management systems practices. For types of standards see reference.
http://www.nist.gov/standardsgov/definestandards.cfm

Standards & Interoperability Framework (S&I Framework)
A collaborative community of participants from the public and private sectors who are focused on providing the tools, services and guidance to facilitate the functional exchange of health information.
http://www.siframework.org/whatis.html

Standards Development Organization (SDO)
SDOs are member-based organizations whose members set the priorities for which standards will be developed and refined. Each SDO has a very refined process for developing, balloting, piloting, finalizing and maintaining standards within its domain. *Note: for this interoperability roadmap, the term is used as defined in this glossary.*

State Innovation Models (SIM) Initiative
The State Innovation Models Initiative is providing support to states for the development and testing of state-based models for multi-payer payment and health care delivery system transformation with the aim of improving health system performance for residents of participating states.
http://innovation.cms.gov/initiatives/state-innovations

Statewide HIE Cooperative Agreement Program
HITECH Act program that funded states' efforts to rapidly build capacity for exchanging health information across the health care system both within and across states.
http://www.healthit.gov/policy-researchers-implementers/state-health-information-exchange

Structured Data Capture (SDC)
An initiative to develop and validate a standards-based data architecture so that a structured set of data can be accessed from EHRs and be stored for merger with comparable data for other relevant purposes like case reports and incident report.
http://wiki.siframework.org/Structured+Data+Capture+Initiative

Systematized Nomenclature of Medicine--Clinical Terms (SNOMED-CT)
SNOMED CT is a comprehensive clinical terminology that was originally developed by the American College of Pathologists. In 2007, the International Health Terminology Standards Development Organisation (IHTSDO), an international SDO, took over SNOMED CT and currently owns, maintains and distributes the vocabulary. The National Library of Medicine (NLM) is the U.S. representative to IHTSDO and is therefore responsible for producing the US edition of SNOMED CT and distributing SNOMED CT in the U.S. It is one of a suite of designated standards for use in U.S. Federal Government systems for the electronic exchange of clinical health information. Meaningful use stage 2 requires that problems be

captured and represented in SNOMED CT when exchanged in the C-CDA. NLM, CMS and other stakeholders are working to enhance the SNOMED CT terminology to include more codes to meet specific semantic needs.
http://www.nlm.nih.gov/research/umls/Snomed/snomed_main.html

Transition of Care (ToC)
The movement of a patient from one setting of care (hospital, ambulatory primary care practice, ambulatory specialty care practice, long-term care, home health, rehabilitation facility) to another.
http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/8_Transition_of_Care_Summary.pdf

Unified Code for Units of Measure (UCUM)
The Unified Code for Units of Measure is a code system intended to include all units of measures being contemporarily used in international science, engineering and business.
http://unitsofmeasure.org/trac/

Unique Ingredient Identifier (UNII)
The UNII is a non- proprietary, free, unique, unambiguous, non-semantic, alphanumeric identifier based on a substance's molecular structure and/or descriptive information.
http://www.fda.gov/ForIndustry/DataStandards/SubstanceRegistrationSystem-UniqueIngredientIdentifierUNII/

Universal Description Discovery and Integration (UDDI)
UDDI specifications form the necessary technical foundation for publication and discovery of Web services implementations both within and between enterprises.
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=uddi-spec

Value Set Authority Center (VSAC)
The Value Set Authority Center (VSAC) is provided by the National Library of Medicine (NLM), in collaboration with the Office of the National Coordinator for Health Information Technology and the Centers for Medicare & Medicaid Services. The VSAC provides downloadable access to all official versions of vocabulary value sets contained in the 2014 Clinical Quality Measures (CQMs). Each value set consists of the numerical values (codes) and human-readable names (terms), drawn from standard vocabularies such as SNOMED CT®, RxNorm, LOINC and ICD-10-CM, which are used to define clinical concepts used in clinical quality measures (e.g., patients with diabetes, clinical visit). The content of the VSAC will gradually expand to incorporate value sets for other use cases, as well as for new measures and updates to existing measures.
https://vsac.nlm.nih.gov/

View online, Download and Transmit (VDT)
One of the Stage 2 Meaningful Use Core Measures under the CMS EHR Incentive Programs is to, "provide patients the ability to view online, download and transmit their health information within four business days of the information being available to the eligible professional."
http://www.healthit.gov/providers-professionals/achieve-meaningful-use/core-measures-2/patient-ability-electronically-view-download-transmit-vdt-health-information

Virtual Private Networks (VPN)
A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer or Wi-Fi-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.
http://en.wikipedia.org/wiki/Virtual_private_network

World Health Organization (WHO)
The directing and coordinating authority for health within the United Nations system that also develops and maintains the International Classification of Diseases (ICD) terminology as the standard diagnostic tool for epidemiology, health management and clinical purposes.
http://www.who.int/classifications/icd/en/

Appendix H: Priority Interoperability Use Cases

A use case is a descriptive statement that defines a scope (or boundary), interactions (or relationships) and specific roles played by actors (or stakeholders) to achieve a goal. The methodology is commonly used to support the identification of requirements and is a simple way to describe the functionalities or needs of an organization.

The following is a list of the priority use cases for nationwide interoperability most commonly submitted to ONC by public and private stakeholders prior to release of the draft Roadmap. Coordinated governance processes should help refine and prioritize this list to then prioritize development of technical standards, policies and implementation specifications.

1. Public health agencies routinely use data derived from standards -based connections with HIEs and EHRs and uses it to plan investments in public health activities.
2. Clinical settings and public health are connected through bi-directional interfaces that enable seamless reporting to public health departments and seamless feedback and decision support from public health to clinical providers.
3. The status of transitions of care should be available to sending and receiving providers to enable effective transitions and closure of all referral loops.
4. Federal, State, provider and consumer use of standardized and interoperable patient assessment data to facilitate coordinated care and improved outcomes.
5. Population health measurement is supported at the community level and includes data from all relevant sources on each patient in the population and is accessible to providers and other stakeholders focused on improving health.
6. Providers and their support staff should be able to track all orders, including those leaving their own organization and EHR, to completion.
7. Individuals integrate data from their health records into mobile apps and tools that enable them to better set and meet their own health goals.
8. CEHRT should be required to provide standardized data export and import capabilities to enable providers to change software vendors.
9. Providers should be alerted or have access to notifications that their attributed patients have had an ER visit, or an admission to or discharge from a hospital.
10. Quality measures are based on complete patient data across multiple sources.
11. Narrative components of the medical record are preserved for provider and patient use and augmented with metadata to enable effective storage, routing and searching for these documents.
12. Providers are able to access x-rays and other images in addition to the reports on patients they are treating, regardless of where the films were taken or housed.
13. Providers and patients have access to genomics testing and data which, when combined with clinical information about patient goals allows the personalization of care and therapies.

14. Patients routinely engage in healthcare encounters using electronic communications such as eVisits and telemedicine.
15. Researchers are able to use de-identified clinical and claims data from multiple sources with robust identity integrity.
16. Patients are routinely offered participation in clinical trials that are relevant to their particular needs and situation.
17. Patients receive alerts and reminders for preventive screenings, care and medication regimens in a manner convenient to and configurable by the patient
18. Patients have the ability to access their holistic longitudinal health record when and where needed.
19. Patients audit their medical records, providing amendments and corrections and supplying missing data such as health outcomes.
20. Patients, families and caregivers are able to use their personal devices such as smartphones, home BP cuffs, glucometers and scales to routinely contribute data to their longitudinal health records and use it or make it available to providers to support decision-making.
21. Patients have access to and can conveniently manage all relevant consents to access or use their data.
22. Those who pay for care use standardized transactions and interoperability to acquire data needed to justify payment
23. Payers should be able to receive notification automatically though the health IT system when a beneficiary is admitted to the hospital.
24. Benefits communication needs to be standardized and made available on all plans through HIT to providers and patients as they make health and healthcare decisions, in a workflow convenient to the decision-making process.
25. Payer/purchaser requirements for payment, such as prior authorization, are clear to the provider at time of order and transacted electronically and timely to support efficient care delivery.
26. All providers in a care team will have unique access, authorization and auditing functionality from health IT systems necessary to fulfill their role on the care team.
27. Data for disease surveillance, immunization tracking and other public health reporting are exchanged automatically.
28. All health IT should provide access and support for disabled users including patients and providers.
29. Query-based exchange should support impromptu patient visits in all settings.
30. Community systems electronically track and report shared risk pool data measures in support of payment reform and delivery
31. Payers use integrated data from clinical and administrative sources to determine reimbursement in support of payment reform
32. Individuals are identified to participate in research opportunities through health data interoperability
33. Providers have the ability to query data from other sources in support of care coordination (patient generated, other providers, etc.) regardless of geography or what network it resides in
34. Providers use genomic data to achieve personalized care

35. Individuals have electronic access to an aggregated view of their health information including their immunization history
36. Individuals integrate data from their health records into apps and tools that enable them to better set and meet their own health goals
37. Individuals regularly contribute information to their electronic health records for use by members of their care team
38. Provider systems electronically track and report high-value measures in support of payment reform and delivery
39. Primary care providers share a basic set of patient information with specialists during referrals; specialists "close the information loop" by sending updated basic information back to the primary care provider
40. Hospitals automatically send an electronic notification and care summary to primary care providers when their patients are discharged
41. Providers and patients receive electronic laboratory results from laboratory information systems (LISs) inside and outside their organization
42. Providers can query or access case management information about patients' care in outside organizations
43. System users have access to provider directory information that is developed to support healthcare communications as well as other use cases
44. Providers have ability to access information in PDMP systems before prescribing narcotics to patients
45. Care providers have electronic access to the information they need for the detection of domestic violence or child abuse
46. Authorized individuals have access to audit logs to ensure appropriate use
47. Disaster relief medical staff members have access to necessary and relevant health information so that they may provide appropriate care to individuals during an emergency
48. Patients routinely engage in mental health risk assessments using electronic communications such as eVisits and telemedicine
49. Emergency medical providers have the ability to query data from other sources while managing chronically ill patients after a disaster regardless of geography or what network the data resides in
50. Population health measurement is supported at the community level and includes data from all relevant sources on each patient in the population (including information on births, deaths and occupational health hazards) and is accessible to providers and other population health stakeholders
51. Population health measurement is supported at the community level and includes statistical data on smoking cessation programs, new patient medical visits and trauma related incidents in a particular area
52. At-risk patients engage in healthcare monitoring programs which can detect life threatening situations (such as patient down and unresponsive) using at-home monitoring devices and electronic communications such as eVisits and telemedicine
53. Payers review clinical documentation for payment purposes
54. Payers review clinical documentation for approval of services (prior authorization)

55. SSA includes functional criteria in some of the Listings of Impairments (the "Listings") to provide an administrative expediency to screen adult disability claimants who are unable to do any gainful activity without consideration of age, education, and work experience. For claimants who do not meet the criteria in the Listings, SSA uses their functional data to perform residual functional capacity assessment to determine their ability to do work.
56. Individuals exercise their choice for consent and consent management policies and procedures are in place to enable the private and secure electronic exchange of behavioral health data.