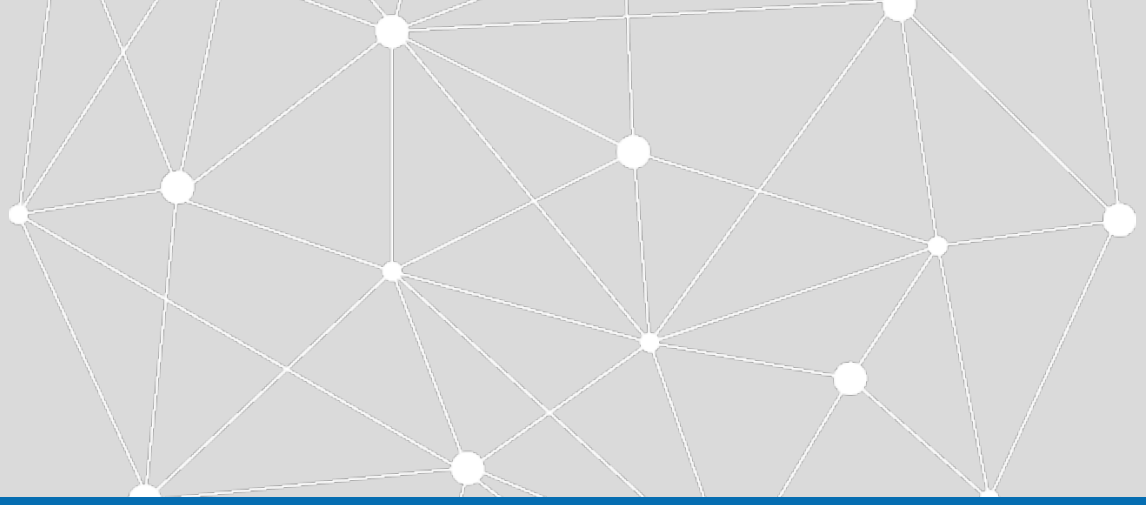

The Trusted Exchange Framework (TEF): Principles for Trusted Exchange

January 2022

This document was published by the U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology and was produced at U.S. taxpayer expense.

This document meets the requirement in section 3001(c)(9)(C) of the Public Health Service Act for the National Coordinator for Health Information Technology to publish on the Office of the National Coordinator for Health Information Technology's public Internet website, and in the Federal Register, the trusted exchange framework (42 U.S.C. 300jj-11(c)(9)(C)).

CONTENTS

Overview and Background

The 21st Century Cures Act[1] (Cures Act) directs the National Coordinator to "develop or support a trusted exchange framework, including a common agreement among health information networks nationally." In January 2018, the Office of the National Coordinator for Health Information Technology (ONC) released the first draft of the Trusted Exchange Framework[2] (TEF Draft 1) for public comment. The TEF Draft 1 included two parts: "Part A — Principles for Trusted Exchange," and "Part B — Minimum Required Terms and Conditions for Trusted Exchange." In April of 2019, ONC released the second draft of the TEF (TEF Draft 2) for public comment, which also included "Part A — Principles for Trusted Exchange" and "Part B — Minimum Required Terms and Conditions for Trusted Exchange."

This document represents the final version of the Trusted Exchange Framework (TEF), titled "The Trusted Exchange Framework: Principles for Trusted Exchange." The policies formerly known as the Minimum Required Terms and Conditions (MRTCs) and the Additional Required Terms and Conditions (ARTCs) are now combined into the Common Agreement. The Common Agreement may be viewed in the Federal Register, on ONC's website, and on the website of The Sequoia Project, Inc., the current entity selected through a competitive process by ONC to serve as the Recognized Coordination Entity (RCE) under a cooperative agreement.[3]

The TEF describes a common set of non-binding, foundational principles for trust policies and practices that can help facilitate exchange among health information networks (HINs). Broad industry alignment with these principles should help facilitate entities' entering into effective contractual relationships for the secure electronic flow of digital health information where and when it is needed. The TEF principles also support the ability of patients (or their legal representatives, which may include caregivers), their health care providers, and other authorized health care stakeholders to electronically access digital health information when and where it is needed most to improve care coordination and quality improvement.

The TEF is built on policy principles that have underpinned ONC's activities and federal health IT policies for over a decade. HINs already follow many of these principles. The inclusion of these principles in the TEF provides a means to further advance their use.

[1] Pub. L. 114–255 (Dec. 13, 2016).
[2] https://www.healthit.gov/sites/default/files/draft-trusted-exchange-framework.pdf.
[3] https://www.healthit.gov/sites/default/files/page/2019-04/TEFCANOFO%20.pdf.

Principles for Trusted Exchange

Principle 1 — Standardization: HINs should prioritize federally recognized and industry recognized technical standards, policies, best practices, and procedures.

A. HINs should prioritize health information technology standards for interoperability that the U.S. Department of Health & Human Services (HHS) has adopted in regulations, ONC has identified in the Interoperability Standards Advisory (ISA), or a standards developing organization (SDO) accredited by the American National Standards Institute (ANSI) has published.

Even where a statute or regulation does not require it, trusted exchange efforts should adhere to federally adopted health information technology standards for interoperability to support robust and widespread adoption. HINs should first look to use standards adopted by HHS for use in Health Insurance Portability and Accountability Act (HIPAA) transactions [4] or use in the ONC Health IT Certification Program [5] (Certification Program), including any updated versions of such adopted standards that ONC has approved for use in the Certification Program through the Standards Version Advancement Process (SVAP), [6] and then those identified in the ISA. [7]

In instances where none of the above references include applicable standards, HINs should then consider voluntary consensus or industry standards that are readily available to all stakeholders and published by SDOs accredited by ANSI. Consistent adherence to standards in the manner described in this paragraph will support improved usability and electronic access to digital health information.

B. HINs should implement technology in a manner that makes it easy to use and allows authorized users to connect to data sources, innovate, and use data to support better, more person-centered care, smarter spending, and healthier people.

HINs should use standards-based technology to electronically exchange digital health information within their own HINs and with other HINs. To minimize variation in how standards are implemented, such technology should be implemented in accordance with authoritative implementation specifications and

[4] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Patient Protection and Affordable Care Act administrative simplification of electronic data interchange provisions are implemented by HHS through the National Standards Group at the Centers for Medicare and Medicaid Services (CMS), which adopts certain transaction standards that are required to be used when electronic data are exchanged in support of covered administrative transactions. These transactions include: health care claims or equivalent encounter information; eligibility for a health plan; enrollment and disenrollment in a health plan; health care electronic funds transfers (EFT) and remittance advice; referral certification and authorizations; health care claims status; coordination of benefits; health plan premium payments; and Medicaid pharmacy subrogation. HIPAA covered entities must use the adopted standards, generally either an ASC X12N or NCPDP standard (for certain pharmacy transactions), in conducting transactions.

[5] *https://www.healthit.gov/topic/certification-ehrs/about-onc-health-it-certification-program*.

[6] ONC Standards Version Advancement Process, *available at https://www.healthit.gov/topic/standards-version-advancement-process-svap*.

[7] ONC Interoperability Standards Advisory (ISA), *available at* https://www.healthit.gov/isa/.

best practices published by an applicable SDO. By doing so, HINs should be better able to connect to each other and with their participants.

HINs should, to the extent possible, ensure that the data exchanged within their own network and with other HINs meets minimum quality standards by using testing and onboarding programs to verify minimum quality levels. HINs may consider using tools to support this analysis, such as ONC's Consolidated Clinical Document Architecture (C-CDA) Scorecard tool for testing the technical conformance of C-CDAs[8] and ONC's Inferno Program Edition tool[9] for testing Fast Healthcare Interoperability Resources (FHIR®) APIs.

Principle 2 — Openness and Transparency: HINs should conduct activities openly and transparently, wherever possible.

A. HINs should make terms, conditions, and contractual agreements that govern the exchange of digital health information easily and publicly available.

All parties desiring to electronically exchange digital health information through a HIN should know, prior to engaging with a HIN, the responsibilities of being a participant in that HIN, the information privacy and security protections the HIN requires, as well as its data use and disclosure policies. HINs should make these and other terms and conditions for participating in their network easily and publicly available, meaning readily found on their websites.

B. HINs should specify and have all of its participants agree to the uses and disclosures for exchanging digital health information.

Because HINs are often either HIPAA business associates of covered entities or a business associate subcontractor of a business associate, their Business Associate Agreements (BAAs) specify the uses and disclosures for which their HIN may be used to electronically exchange digital health information.[10] While some HINs currently support many of the uses and disclosures specifically addressed in the HIPAA Privacy Rule,[11] others may only support use and disclosure of digital health information for treatment purposes.

When HINs vary in allowable uses and disclosures in their agreements, the full electronic exchange of digital health information between those HINs is limited. Therefore, HINs should, in compliance with applicable law, specify the minimum set of uses and disclosures they support. These uses and disclosures should be specified in a HIN's legal agreement with its participants or included in a contract addendum if the legal agreement is already in place, made open and transparent, consistent with Principle 2.A, and

[8] ONC Consolidated-Clinical Document Architecture (C-CDA) Scorecard, https://site.healthit.gov/home.
[9] ONC Inferno Program Edition, https://inferno.healthit.gov/inferno/.
[10] For information about HIPAA covered entities and business associates, *see* 45 CFR 160.103 and https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.
[11] The "HIPAA Privacy Rule" refers to the privacy regulations under HIPAA, 45 CFR part 160 and subparts A and E of part 164.

clearly communicated to relevant parties prior to when digital health information[12] is requested or sent between participants and HINs.

C. HINs should publish, keep current, and make publicly available the HIN's privacy practices.

Ensuring that participants of HINs understand the privacy practices of each HIN will help to build trust that digital health information will be protected and will not be used in ways that they do not expect. Consequently, HINs and their participants should subscribe to the following privacy practices:

(a) HINs must comply with all applicable laws and regulations regarding the use and disclosure of digital health information. When consent or authorization is required by federal or state law, HINs should have policies for where consent and/or authorization is enforced within their architecture.
(b) HINs should clearly specify the minimum set of uses and disclosures for exchanging digital health information and, for non-treatment purposes, limit the use of digital health information to the minimum amount required.
(c) HINs should advance the ability of individuals to electronically access their digital health information through HINs' privacy practices.

These privacy practices are critical to effective data exchange. To further promote transparency, HINs should publish and make publicly available a notice written in plain language, similar to ONC's Model Privacy Notice,[13] that describes their privacy practices regarding the access, exchange, use, and disclosure of digital health information.

D. HINs should establish and, where applicable, conduct any dispute resolution processes in an equitable and transparent manner.

It may be necessary to address behavior that violates data sharing agreements among HINs. HINs should ensure that a dispute resolution process for addressing such violations is clearly defined in their respective agreements and subsequently followed. Such dispute resolution processes should be equitable and transparent to all parties, particularly prior to when a data sharing entity signs an agreement with a HIN that binds that entity to such processes.

---

[12] The term "digital" when used throughout this document has its plain meaning (i.e., its dictionary definition). *See* Merriam-Webster.com., *https://www.merriam-webster.com/dictionary/digital* (retrieved Jan. 7, 2022). For example, the phrase "digital health information" refers to information that is neither faxed nor is hard copy health information. Furthermore, the phrase "digital health information" is used to deliberately avoid use of specific regulatory terms for specific types of health information.

[13] ONC Model Privacy Notice, *available at www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf*.

Principle 3 — Cooperation and Non-Discrimination: HINs should collaborate with stakeholders across the continuum of care to electronically exchange digital health information, even when a stakeholder may be a business competitor.

HINs should not seek to gain competitive advantage or discriminate against competitors by limiting access to individuals' digital health information, and HINs should not treat digital health information as an asset that can be restricted in order to obtain or maintain a competitive advantage. For example, HINs should not withhold digital health information requested for permitted treatment, payment, or health care operations purposes from health care providers or health plans that are outside of their preferred referral networks or outside of a value-based payment arrangement. They should not establish internal policies and procedures that result in such improper withholding of information. Likewise, HINs should not implement technology in a manner that improperly limits the sharing of digital health information. HINs should not knowingly make misleading statements regarding privacy or security laws or regulations as a pretext for not sharing digital health information. HINs should practice data reciprocity (e.g., have a willingness to share digital health information themselves as opposed to participating in an exchange relationship only for the purpose of receiving digital health information from others). In addition, fees and other costs should be reasonable and should not be used to interfere with access, exchange, use, or disclosure of digital health information within a HIN or between HINs.

HINs should not use contract provisions or proprietary technology implementations to unduly limit connectivity with other HINs—such as by preventing the appropriate flow of digital health information across technological, geographic, or organizational boundaries for health and care, safety, quality measurement, or payment. At the same time, HINs are subject to applicable law, which includes restrictions or policies that interact with such potential limits to connectivity (including the applicable HIPAA Rules[14] and information blocking regulations[15]).

HINs should not use methods that discourage or impede appropriate digital health information exchange with competitors or potential competitors. This includes throttling the speed with which data is exchanged purely for competitive reasons, unnecessarily limiting the data that are exchanged with health care organizations that may be their competitor or a competitor of one of their participants, or requiring unnecessary testing requirements designed to unfairly deter or discourage connections that do not benefit the HIN.

[14] The term "HIPAA Rules" refers to the HIPAA Privacy, Security, and Breach Notification Rules, 45 CFR parts 160 and 164.
[15] *See* 45 CFR part 171.

Principle 4 — Privacy, Security, and Safety: HINs should exchange digital health information in a manner that supports privacy; ensures data confidentiality, integrity, and availability; and promotes patient safety.

A. HINs should ensure that digital health information is exchanged and used in a manner that promotes safe care and wellness, including consistently and accurately matching digital health information to an individual.

Health plans and most health care providers, and their business associates must follow the HIPAA Rules to safeguard health information. However, digital health information is increasingly collected, shared, or used by new types of organizations that are beyond the traditional health care organizations covered by the HIPAA Rules. Privacy and security should be a foundation for all HINs and HIN participants, including those that are not subject to HIPAA.

Ensuring the confidentiality, integrity, and availability of digital health information is paramount to providing safe care and supporting the health and well-being of all individuals and communities. When digital health information is exchanged, a foundational step to safe care and wellness begins with correctly matching the data to an individual so that care is provided to the correct individual based on accurate information. Generally, sophisticated algorithms that use demographic data for matching are the primary method for automatically connecting data to an individual within a HIN. Demographic data quality heavily influences the accuracy and completeness that any given patient matching method can achieve. To support accurate matching, HINs should agree upon and consistently share a core set of demographic data each time digital health information is exchanged. Likewise, participants of HINs should ensure that the core set of demographic data is consistently captured for all individuals to enable exchange in a standard format and to accurately match patient data. Furthermore, HINs and their participants should also work to improve the quality of the demographic data that they hold.[16]

Where possible, standard nomenclatures should be used and exchanged in a data format that is consumable by a receiving system, such as a C-CDA or via FHIR APIs. Further, clinicians should update individuals' digital health information in their health IT systems to ensure that medications, allergies, and problems are up to date prior to exchanging such data with another organization. HINs should utilize testing and onboarding processes for their participants to establish a high level of data quality.

B. Within the context of applicable law, HINs should enforce policies concerning individuals' ability to consent to the access, exchange, or use of their digital health information.

When consent or authorization is required by federal or state law, HINs should have policies addressing how consent and/or authorization is enforced within their architecture. The ability to oversee appropriate electronic capture of an individual's consent or authorization to access, exchange, or use their digital health information will engender trust with other entities seeking to exchange with that network.

---

[16] ONC's Patient Demographic Data Quality Framework module is intended to support health systems, large practices, health information exchanges, and payers in improving their patient demographic data quality. *See* *https://www.healthit.gov/playbook/pddq-framework/*.

Differing state laws affect when HINs must obtain consent or authorization from an individual to access, exchange, or use the individual's digital health information. The Privacy Rule does not require a covered entity or its business associates to obtain an individual's consent or authorization before using or disclosing health information for treatment, payment, and health care operations purposes. While the Privacy Rule generally permits covered health care providers to request consent for those purposes, some federal and state laws may require them to do so before they disclose or exchange an individual's digital health information even for treatment and payment purposes. For example, in the case of records regarding human immunodeficiency virus (HIV), mental health, or genetic testing, state laws may impose a more stringent standard (e.g., requiring consent from the individual) than the Privacy Rule.[17] Thus, HINs should have policies that are sufficiently flexible to address these differing consent and authorization requirements.

Principle 5 — Access: HINs should ensure that individuals and their authorized caregivers have easy access to their digital health information and understand how it has been used or disclosed and HINs should comply with civil rights obligations on accessibility.

A. HINs should not impede or impose any unnecessary barriers to the ability of individuals or their legal representatives to access or direct their digital health information to designated third parties, or to learn how information about them has been accessed or disclosed.

HINs who maintain digital health information should (1) enable individuals, or their legal representatives, to easily and conveniently access their digital health information; (2) enable individuals, or their legal representatives, to direct their digital health information to any recipient they designate; and (3) ensure that individuals, or their legal representatives, have a way to learn how their information is shared and used. This principle is consistent with the Privacy Rule, which generally requires covered entities to provide health information to individuals in the form and format in which they request it, if it is readily producible in that form and format.

The Privacy Rule also requires a covered entity to have a Notice of Privacy Practices available to inform individuals about how health information is used and disclosed by the entity, as well as the individual's rights with respect to their health information.

In accordance with applicable law, HINs should support an individual's decision to access their digital health information through an API-enabled third-party application when the individual has directed the HIN to disclose a copy of that individual's health information to the application.

[17] Privacy and Security Solutions for Interoperable Health Information Exchange, Report on State Law Requirements for Patient Permissions to Disclose Health Information (Aug. 2009), *https://www.healthit.gov/sites/default/files/disclosure-report-1.pdf*.

In accordance with federal law, HINs that receive federal funding must ensure accessibility by individuals with disabilities and individuals with limited English proficiency.[18]

B. HINs should not impede or impose any unnecessary barriers to the ability of individuals, or their legal representatives, to learn how their health data has been accessed or disclosed.

It is important for individuals, or their legal representatives, to be able to obtain information about how their digital health information has been accessed, used, and disclosed. As the Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information states in its principle on "Openness and Transparency," "[p]ersons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should provide reasonable opportunities for individuals to review who has accessed their individually identifiable health information or to whom it has been disclosed, in a readable form and format."[19]

HINs should commit to following this principle and should provide such opportunities to review access histories electronically whenever possible, particularly when an individual makes the request electronically. Providing individuals with transparency on how their data has been accessed, used, and disclosed increases their confidence in the HIN.[20] Again, in accordance with federal law, HINs that receive federal funding must ensure accessibility.

Principle 6 — Equity: HINs should consider the impacts of interoperability on different populations and throughout the lifecycle of the activity.

A. HINs should employ a health equity by design approach and should consider the health equity consequences of policy and technology choices up front.

HINs should adopt standards, policies, and processes that explicitly consider health equity.[21] The COVID-19 pandemic amplified the importance of health equity in health IT. Throughout the pandemic,

---

[18] *See, e.g.,* Title VI of the Civil Rights Act of 1964, 42 U.S.C. §§ 2000d-2000d-7 and its implementing regulation at 45 CFR part 80; Section 1557 of the Patient Protection and Affordable Care Act, 42 U.S.C. 18116, and its implementing regulation at 45 CFR part 92; and Section 504 of the Rehabilitation Act of 1973, 29 U.S.C. 794, and its implementing regulation at 45 CFR part 84.

[19] Office of the National Coordinator for Health Information Technology, Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information, at 7 (Dec. 15, 2008), *available at* http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf.

[20] *See* Privacy and Security Solutions for Interoperable Health Information Exchange, Report on State Law Requirements for Patient Permissions to Disclose Health Information (Aug. 2009), https://www.healthit.gov/sites/default/files/disclosure-report-1.pdf.

[21] Exec. Order No. 13985, Advancing Racial Equity and Support for Underserved Communities Through the Federal Government, available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/executive-order-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government/. This Executive Order defines equity as "the consistent and systematic fair, just, and impartial treatment of all

public health authorities faced challenges in receiving the granular data needed on specific communities because of inconsistent and heterogeneous data collection and exchange across public health systems. Organizations on the frontline were often unable to get sufficient information needed for decision-making to support a targeted public health response.

A health equity by design approach means that HINs should identify the health equity considerations at the outset of any policy creation, technology development process, or implementation approach, and should include those as core constructs to identify and address health inequities and disparities.

B. HINs should evaluate interoperability efforts, ensure health equity is being achieved, and adjust when it is not.

Evaluation and analysis provide essential evidence to understand how programs work, for whom, and under what circumstances.[22] Building evidence through evaluation and analysis informs decisions in a range of areas, including budget formation, regulatory development, strategic planning, program implementation, and policy construction.[23]

HINs should plan and budget for evaluation of their trusted exchange efforts during all stages of an exchange activity's life cycle. Such evaluation should follow best practices including, for example, the Centers for Disease Control and Prevention Framework for Program Evaluation in Public Health.[24] Additionally, as part of continuous quality improvement activities,[25, 26, 27] HINs should consider the results of such ongoing evaluation and make changes to improve outcomes, including changes in the domain of equity.

---

individuals, including individuals who belong to underserved communities that have been denied such treatment, such as Black, Latino, and Indigenous and Native American persons, Asian Americans and Pacific Islanders, and other persons of color; members of religious minorities; lesbian, gay, bisexual, transgender, and queer (LGBTQ+) persons; persons with disabilities; persons who live in rural areas; and persons otherwise adversely affected by persistent poverty or inequality."

[22] Adapted from HHS Office of the Assistant Secretary for Planning and Evaluation, Evaluation & Evidence, *https://aspe.hhs.gov/evaluation-evidence*.

[23] *Id.*

[24] Centers for Disease Control and Prevention, *Framework for Program Evaluation in Public Health*, Morbidity and Mortality Weekly Report, Vol. 48, No. RR-11 (Sept. 17, 1999*), available at* *https://www.cdc.gov/mmwr/PDF/rr/rr4811.pdf*.

[25] Brian O'Donnell and Vikas Gupta, Continuous Quality Improvement (last updated Apr. 7, 2021), *available at* *https://www.ncbi.nlm.nih.gov/books/NBK559239/*.

[26] Office of the National Coordinator for Health Information Technology, National Learning Consortium, Continuous Quality Improvement (CQI) Strategies to Optimize your Practice, *https://www.healthit.gov/sites/default/files/tools/nlc_continuousqualityimprovementprimer.pdf*.

[27] Agency for Healthcare Research and Quality, Health Literacy Universal Precautions Toolkit, 2nd Edition, Plan-Do-Study-Act (PDSA) Directions and Examples, *available at* *https://www.ahrq.gov/health-literacy/improve/precautions/tool2b.html*.

Principle 7 — Public Health: HINs should support public health authorities and population-level use cases to enable the development of a learning health system that improves the health of the population and lowers the cost of care.

A. HINs should enable use cases that advance the mission of public health authorities.

Currently, nationwide networks largely support exchange among health care providers for treatment purposes to the exclusion of other critical use cases such as public health, population health, and research. Whenever possible, and in accordance with applicable law, HINs should support use cases that advance priorities for public health authorities.[28, 29] This includes, for example, electronic case reporting, electronic laboratory reporting, case investigations, syndromic surveillance, immunization reporting, adverse event collection or reporting, product defects, product recalls, and post-marketing surveillance.[30, 31]

B. HINs should advance population-level use cases, including quality improvement and research.

Population-level information is fundamental to providing accountability for health care and to enabling a learning health system. A learning health system is defined as a health system in which internal data and experience are systematically integrated with external evidence, and that knowledge is put into practice.[32] As a result, patients get higher quality, safer, more efficient care, and health care delivery organizations become better places to work.[33]

In alignment with Principle 3.A., HINs should enable data exchange for quality measurement and improvement activities. Providers and health plans may want to work with a HIN, consistent with applicable law, to share digital health information from their health information technology to a qualified

---

[28] A "public health authority" is an agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency. *See* 45 CFR 164.501. Examples of a public health authority include State and local health departments, the U.S. Food and Drug Administration (FDA), the Centers for Disease Control and Prevention, and the Occupational Safety and Health Administration (OSHA). Generally, covered entities are required reasonably to limit the protected health information disclosed for public health purposes to the minimum amount necessary to accomplish the public health purpose. However, covered entities are not required to make a minimum necessary determination for public health disclosures that are made pursuant to an individual's authorization, or for disclosures that are required by other law. *See* 45 CFR 164.502(b). For additional information, *see* https://www.hhs.gov/hipaa/for-professionals/special-topics/public-health/index.html.

[29] Office of the National Coordinator for Health Information Technology, Public Health, https://www.healthit.gov/topic/health-it-health-care-settings/public-health.

[30] Centers for Disease Control and Prevention, Public Health Data Interoperability, https://www.cdc.gov/datainteroperability/index.html.

[31] HHS Office of Civil Rights, Public Health, https://www.hhs.gov/hipaa/for-professionals/special-topics/public-health/index.html.

[32] HHS Agency for Healthcare Research and Quality, About Learning Health Systems (last reviewed May 2019), https://www.ahrq.gov/learning-health-systems/about.html.

[33] *Id.*

clinical data registry (QCDR),[34] a qualified entity (QE),[35] researchers, another HIN, or a health IT developer providing care coordination or quality measurement services. Health plans, including employer-sponsored group health plans, may wish to work with HINs to, where appropriate, obtain information that would better support operations, including using analytics for services such as assessing individuals' risk, population health analysis, and quality and cost analyses.

HINs should support biomedical research activities where appropriate and permitted by law. Under the Cures Act, the Secretary is required to establish a program to evaluate the potential use of real-world evidence to help support the approval of a new indication for drugs and to help to support or satisfy post-approval study requirements.[36] The U.S. Food and Drug Administration uses real-world data and real-world evidence to monitor postmarket safety and adverse events and to make regulatory decisions.[37] To support these and other related use cases, HINs should support biomedical research through their trusted exchange activities, where appropriate. As with all data access supported by HINs, research use cases must always be conducted in accordance with applicable law, guidelines, and ethical principles and considerations.

[34] A Qualified Clinical Data Registry (QCDR) is a CMS-approved vendor that is in the business of improving health care quality. These organizations may include specialty societies, regional health collaboratives, and large health systems or software vendors working in collaboration with one of these medical entities. *See* https://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-instruments/MMS/Downloads/A-Brief-Overview-of-Qualified-Clinical-Data-Registries.pdf.

[35] The CMS Qualified Entity (QE) Program, also known as the Medicare Data Sharing for Performance Measurement Program, enables organizations to receive Medicare claims data under parts A, B, and D for use in evaluating provider performance. Organizations approved as QEs are required to use the Medicare data to produce and publicly disseminate CMS-approved reports on provider performance. *See* https://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/QEMedicareData.

[36] Pub. L. 114-255, section 505F.

[37] U.S. Food and Drug Administration, Real World Evidence (content current as of Sept. 30, 2021), https://www.fda.gov/science-research/science-and-research-special-topics/real-world-evidence.