Self-Assessment

Patient Identification

General Instructions for the SAFER Self-Assessment Guides

The SAFER Guides are designed to help healthcare organizations conduct self-assessments to optimize the safety and safe use of electronic health records (EHRs) in the following areas.

- High Priority Practices
- Organizational Responsibilities
- Contingency Planning
- System Configuration
- System Interfaces
- Patient Identification
- Computerized Provider Order Entry with Decision Support
- Test Results Reporting and Follow-up
- Clinician Communication

Each of the nine SAFER Guides begins with a Checklist of "recommended practices." The downloadable SAFER Guides provide fillable circles that can be used to indicate the extent to which each recommended practice has been implemented. Following the Checklist, a Practice Worksheet gives a rationale for and examples of how to implement each recommended practice, as well as likely sources of input into assessment of each practice, and fillable fields to record team members and follow-up action. In addition to the downloadable version, the content of each SAFER Guide, with interactive references and supporting materials, can also be viewed on ONC's website at www.healthit.gov/SAFERGuide.

The SAFER Guides are based on the best evidence available at this time (2016), including a literature review, expert opinion, and field testing at a wide range of healthcare organizations, from small ambulatory practices to large health systems.

The recommended practices in the SAFER Guides are intended to be useful for all EHR users. However, every organization faces unique circumstances and will implement a particular practice differently. As a result, some of the specific examples in the SAFER Guides for recommended practices may not be applicable to every organization.

The SAFER Guides are designed in part to help deal with safety concerns created by the continuously changing landscape that healthcare organizations face. Therefore, changes in technology, practice standards, regulations and policy should be taken into account when using the SAFER Guides. Periodic self-assessments using the SAFER Guides may also help organizations identify areas in which it is particularly important to address the implications of change for the safety and safe use of EHRs. Ultimately, the goal is to improve the overall safety of our health care system.

The SAFER Guides are not intended to be used for legal compliance purposes, and implementation of a recommended practice does not guarantee compliance with HIPAA, the HIPAA Security Rule, Medicare or Medicaid Conditions of Participation, or any other laws or regulations. The SAFER Guides are for informational purposes only and are not intended to be an exhaustive or definitive source. They do not constitute legal advice. Users of the SAFER Guides are encouraged to consult with their own legal counsel regarding compliance with Medicare or Medicaid program requirements, HIPAA, and any other laws.

For additional, general information on Medicare and Medicaid program requirements, please visit the Centers for Medicare & Medicaid Services website at www.cms.gov. For more information on HIPAA, please visit the HHS Office for Civil Rights website at www.hhs.gov/ocr.

Self-Assessment

Patient Identification

Introduction

The *Patient Identification SAFER Guide* identifies recommended safety practices associated with the reliable identification of patients in the EHR. Accurate patient identification ensures that the information presented by and entered into the EHR is associated with the correct person. Processes related to patient identification are complex and require careful planning and attention to avoid errors. In the EHR-enabled healthcare environment, providers rely on technology to help support and manage these complex identification processes. Technology configurations alone cannot ensure accurate patient identification.[1] Staff also must be supported with adequate training and reliable procedures.

This self-assessment can help identify and evaluate where breakdowns related to patient identification occur in the healthcare setting. The self-assessment focuses on processes within organizations related to the creation of new patient records, patient registration, retrieval of information on previously registered patients, and other types of patient identification activities. The recommended practices can help prevent or detect and mitigate problems caused by duplicate records, patient mix-ups, and "comingled" (or "overlay") records.[2, 3, 4, 5, 6, 7, 8, 9, 10, 11]

This guide is meant to support and enable patient matching technology and capabilities, focusing on best practices for improving data accuracy, which is the first necessary step to ensuring accurate patient matching. However, patient matching between organizations is not the focus of this guide.

The recommended practices in this Patient Identification SAFER Guide provide support for many, varied patient matching technologies, as well as alternatives and best practices on specific patient attributes for patient matching, which are likely to change over time.

Completing the self-assessment in the Patient Identification SAFER Guide requires the engagement of people both within and outside the organization (e.g., EHR technology developers). Because this guide is designed to help organizations prioritize EHR-related safety concerns, clinician leadership in the organization should be engaged in assessing whether and how any particular recommended practice affects the organization's ability to deliver safe, high quality care. Collaboration between clinicians and staff members while completing the self-assessment in this guide will enable an accurate snapshot of the organization's patient identification status (in terms of safety), and even more importantly, should lead to a consensus about the organization's future path to optimize EHR-related safety and quality: setting priorities among the recommended practices not yet addressed, ensuring a plan is in place to maintain recommended practices already in place, dedicating the required resources to make necessary improvements, and working together to prevent and mitigate the highest priority patient identification-related safety risks introduced by the EHR.

Self-Assessment

Patient Identification

Table of Contents

The SAFER Self-Assessment Guides were developed by health IT safety researchers and informatics experts:

Joan Ash, *PhD, MLS, MS, MBA, Professor and Vice Chair, Department of Medical Informatics and Clinical Epidemiology, School of Medicine, Oregon Health & Science University*;

Hardeep Singh, *MD, MPH, Associate Professor of Medicine at the Michael E. DeBakey Veterans Affairs Medical Center and Baylor College of Medicine and Chief of the Health Policy, Quality and Informatics Program at the Houston VA HSR&D Center of Excellence, and Director of the Houston VA Patient Safety Center of Inquiry; and*

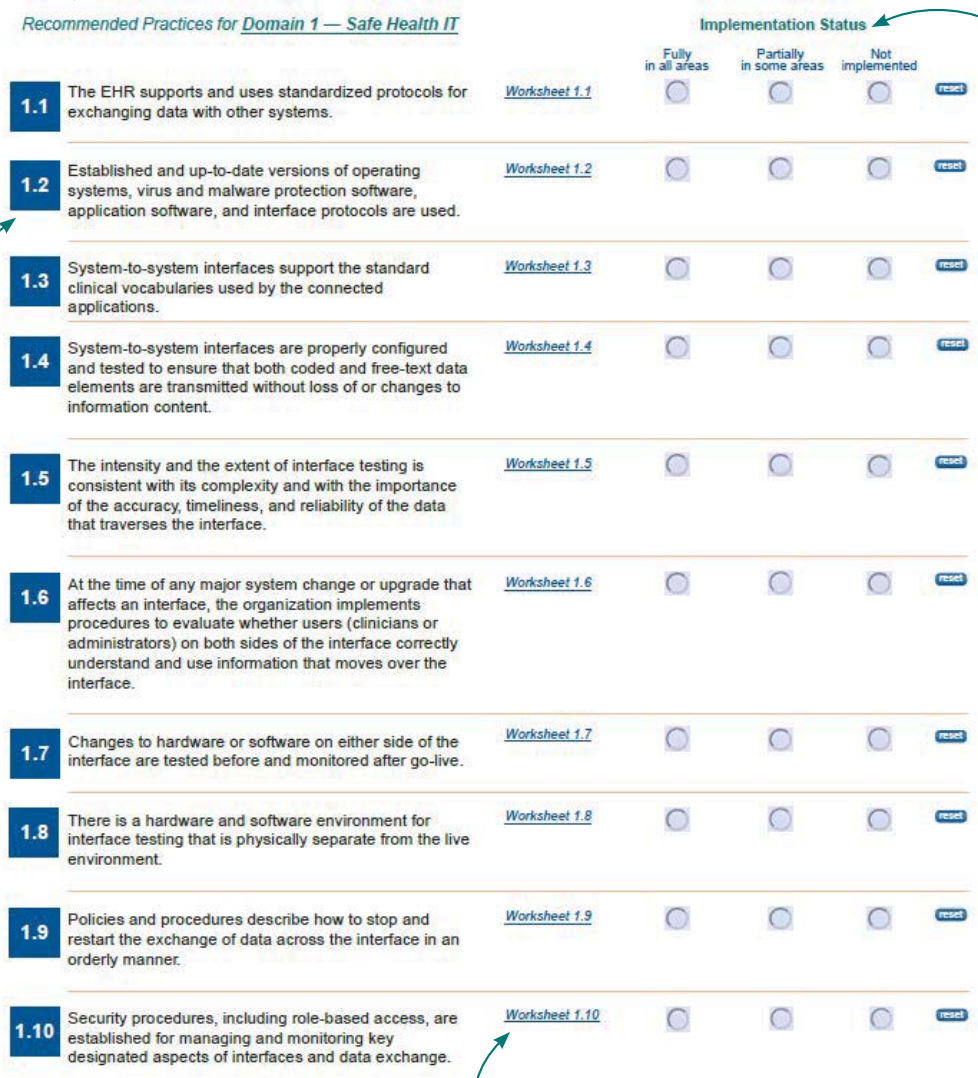
Dean Sittig, *PhD, University of Texas School of Biomedical Informatics at Houston, UT–Memorial Hermann Center for Healthcare Quality & Safety.*

This guide was developed under the contract Unintended Consequences of Health IT and Health Information Exchange, Task Order HHSP23337003T/HHSP23320095655WC.

The *Checklist* is structured as a quick way to enter and print your self-assessment. Your selections on the checklist will automatically update the related section of the corresponding *Recommended Practice Worksheet.*

The *Domain* associated with the *Recommended Practice(s)* appears at the top of the column.

The *Recommended Practice(s)* for the topic appear below the associated *Domain.*



Recommended Practices for Domain 1 — Safe Health IT		Implementation Status: Fully in all areas	Partially in some areas	Not implemented	
1.1 The EHR supports and uses standardized protocols for exchanging data with other systems.	Worksheet 1.1	○	○	○	reset
1.2 Established and up-to-date versions of operating systems, virus and malware protection software, application software, and interface protocols are used.	Worksheet 1.2	○	○	○	reset
1.3 System-to-system interfaces support the standard clinical vocabularies used by the connected applications.	Worksheet 1.3	○	○	○	reset
1.4 System-to-system interfaces are properly configured and tested to ensure that both coded and free-text data elements are transmitted without loss of or changes to information content.	Worksheet 1.4	○	○	○	reset
1.5 The intensity and the extent of interface testing is consistent with its complexity and with the importance of the accuracy, timeliness, and reliability of the data that traverses the interface.	Worksheet 1.5	○	○	○	reset
1.6 At the time of any major system change or upgrade that affects an interface, the organization implements procedures to evaluate whether users (clinicians or administrators) on both sides of the interface correctly understand and use information that moves over the interface.	Worksheet 1.6	○	○	○	reset
1.7 Changes to hardware or software on either side of the interface are tested before and monitored after go-live.	Worksheet 1.7	○	○	○	reset
1.8 There is a hardware and software environment for interface testing that is physically separate from the live environment.	Worksheet 1.8	○	○	○	reset
1.9 Policies and procedures describe how to stop and restart the exchange of data across the interface in an orderly manner.	Worksheet 1.9	○	○	○	reset
1.10 Security procedures, including role-based access, are established for managing and monitoring key designated aspects of interfaces and data exchange.	Worksheet 1.10	○	○	○	reset

Select the level of implementation achieved by your organization for each *Recommended Practice.*

Your *Implementation Status* will be reflected on the *Recommended Practice Worksheet* in this PDF.

To the right of each *Recommended Practice* is a link to the *Recommended Practice Worksheet* in this PDF.

The Worksheet provides guidance on implementing the Practice.

*Recommended Practices for **Domain 1 — Safe Health IT***

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
1.1	An enterprise-wide master patient index that includes patients' demographic information and medical record number (or multiple numbers if used by different parts of the same organization, along with primary number/ key) is used to identify patients before importing data.	*Worksheet 1.1*	○	○	○	reset
1.2	To facilitate correct patient identification, clinicians have the ability to create personalized electronic lists of their patients according to several criteria (e.g., user, location, time, service).	*Worksheet 1.2*	○	○	○	reset
1.3	Information required to accurately identify the patient is clearly displayed on all portions of the EHR user interface, wristbands, and printouts.	*Worksheet 1.3*	○	○	○	reset
1.4	Patient names on adjacent lines in the EHR display are visually distinct.	*Worksheet 1.4*	○	○	○	reset
1.5	Medical record numbers incorporate a "check digit" to help prevent data entry errors.	*Worksheet 1.5*	○	○	○	reset
1.6	Users are warned when they attempt to create a record for a new patient (or look up a patient) whose first and last names are the same as another patient, or attempt to look up a patient and the search returns multiple patients with the same or similar names.	*Worksheet 1.6*	○	○	○	reset

*Recommended Practices for **Domain 2 — Using Health IT Safely***

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
2.1	Patients are registered in a centralized, common database using standardized procedures.	*Worksheet 2.1*	○	○	○	reset
2.2	The user interfaces of the training, test, and read-only backup environments of the EHR are clearly different from the production (i.e., "live") version to prevent inadvertent entry or review of patient information in the wrong system.	*Worksheet 2.2*	○	○	○	reset
2.3	The organization has a process to assign a "temporary" unique patient ID (which is later merged into a permanent ID) in the event that either the patient registration system is unavailable or the patient is not able to provide the required information.	*Worksheet 2.3*	○	○	○	reset

*Recommended Practices for **Domain 2 — Using Health IT Safely***

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
2.4	Patient identity is verified at key points or transitions in the care process (e.g., prior to procedures and surgeries, rooming patient, vital sign recording, order entry, medication administration, check out).	*Worksheet 2.4*	○	○	○	reset
2.5	The EHR limits the number of patient records that can be displayed on the same computer at the same time to one.	*Worksheet 2.5*	○	○	○	reset
2.6	Patients who are deceased are clearly identified as such.	*Worksheet 2.6*	○	○	○	reset
2.7	The use of test patients in the production (i.e., "live") environment is carefully monitored. When they do exist, they have unambiguously assigned "test" names (e.g., including numbers or multiple Z's) and are clearly identifiable as test patients (e.g., different background color for patient header).	*Worksheet 2.7*	○	○	○	reset

*Recommended Practices for **Domain 3 — Monitoring Safety***

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
3.1	The organization regularly monitors its patient database for patient identification errors and potential duplicate patients or records.	*Worksheet 3.1*	○	○	○	reset

A multi-disciplinary team should complete this self-assessment and evaluate potential health IT-related patient safety risks addressed by this specific SAFER Guide within the context of your particular healthcare organization.

This Team Worksheet is intended to help organizations document the names and roles of the self-assessment team, as well as individual team members' activities. Typically team members will be drawn from a number of different areas within your organization, and in some instances, from external sources. The suggested Sources of Input section in each Recommended Practice Worksheet identifies the types of expertise or services to consider engaging. It may be particularly useful to engage specific clinician and other leaders with accountability for safety practices identified in this guide.

The Worksheet includes fillable boxes that allow you to document relevant information. The Assessment Team Leader box allows documentation of the person or persons responsible for ensuring that the self-assessment is completed. The section labeled Assessment Team Members enables you to record the names of individuals, departments, or other organizations that contributed to the self-assessment. The date that the self-assessment is completed can be recorded in the Assessment Completion Date section and can also serve as a reminder for periodic reassessments. The section labeled Assessment Team Notes is intended to be used, as needed, to record important considerations or conclusions arrived at through the assessment process. This section can also be used to track important factors such as pending software updates, vacant key leadership positions, resource needs, and challenges and barriers to completing the self-assessment or implementing the Recommended Practices in this SAFER Guide.

Assessment Team Leader

Assessment Completion Date

Assessment Team Members

Assessment Team Notes

reset page

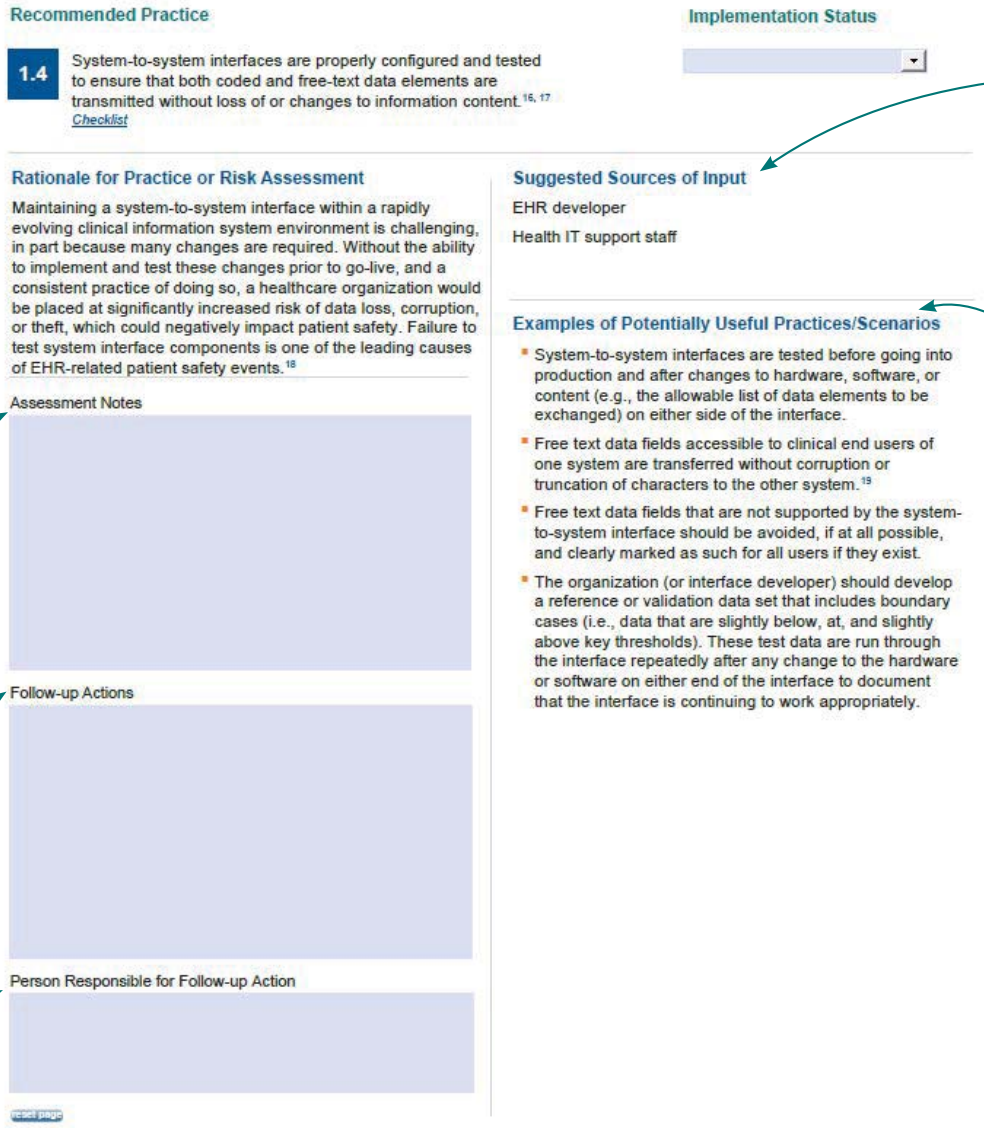
Each *Recommended Practice Worksheet* provides guidance on implementing a specific *Recommended Practice*, and allows you to enter and print information about your self-assessment.

The *Rationale* section provides guidance about "why" the safety activities are needed.

Enter any notes about your self-assessment.

Enter any follow-up activities required.

Enter the name of the person responsible for the follow-up activities.



The *Suggested Sources of Input* section indicates categories of personnel who can provide information to help evaluate your level of implementation.

The *Examples* section lists potentially useful practices or scenarios to inform your assessment and implementation of the specific *Recommended Practice*.

Recommended Practice

1.1 An enterprise-wide master patient index that includes patients' demographic information and medical record number (or multiple numbers if used by different parts of the same organization, along with primary number/key) is used to identify patients before importing data.[12, 13]
Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Duplicate patient records are a common problem and can cause harm when clinicians lack complete information on their patients.[14] Harm can also result when two patients' records are co-mingled. An enterprise-wide master patient index reduces the occurrence of duplicate patient records by increasing the likelihood that patients with previous encounters are identified.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- The master patient index employs a probabilistic matching algorithm that uses patients' first and last names, date of birth, gender, and other attributes (e.g., zip code, telephone number, the last four digits of the Social Security number).[15]
- The organization has policies and procedures to identify and prevent duplicate patient record creation and to integrate unintentional duplicate records into one complete record.[14, 16]
- Organizational policies address how to ensure correct patient identification of information from external sources (e.g., external labs, pharmacies, healthcare providers).
- As new recommended practices are defined, the organization updates its policies and procedures related to the use of the master patient index.[14]

Recommended Practice

1.2 To facilitate correct patient identification, clinicians have the ability to create personalized electronic lists of their patients according to several criteria (e.g., user, location, time, service).[17]
Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Selecting a patient from a shorter list of relevant patients reduces the risk of selecting the wrong patient.[18]

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- Patient lists can be automatically generated in several formats to provide information relevant to a clinical or administrative need: person-specific (e.g., all patients that a clinician is responsible for), location-specific (e.g., all patients on a particular nursing unit or clinic), time-specific (e.g., all patients on today's schedule), and service- or clinician-specific (e.g., all patients being cared for by a particular specialty, service, or clinician).[13]
- Clinicians can view (i.e., read), edit (i.e., write: create, modify, delete), and use (i.e., execute: select a patient) patient lists related to their own clinical purposes.
- Patient lists should by sorted in a clinically relevant order by default (e.g., by room number, appointment time), rather than alphabetically, to reduce the chance of look-alike or sound-alike names appearing close together.[13]
- There are two or more patient identifiers included with each patient on the list (e.g., name, date of birth, medical record number, gender).[13, 19, 20]

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Recommended Practice

1.3 Information required to accurately identify the patient is clearly displayed on all portions of the EHR user interface, wristbands, and printouts.[13, 21]
Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Providing medical services to the wrong patient is a common, preventable source of patient harm.[18, 22] Steps should be taken to ensure that the person using an EHR to care for a patient is addressing the intended patient. Doing so reduces the risk of "wrong patient" errors.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- All computer-generated EHR user interface windows incorporate the following information to facilitate patient identification, with appropriate exceptions for individuals for whom such information could create other risks (e.g., victims of domestic violence):[13]
  - Last name, first name, date of birth (with calculated age)
  - Gender
  - Medical record number
  - In-patient location (or home address or ZIP code)
  - Recent photograph (recommended)
  - Responsible physician (optional)
- Organizational policies and workflows incorporate use of the EHR into ensuring correct patient identification.

Recommended Practice

1.4 Patient names on adjacent lines in the EHR display are visually distinct.[13]
Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Keeping patient names visually distinct in the EHR reduces the likelihood of unintentionally selecting the wrong patient. This is a basic good usability practice.

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- On all patient lists containing two or more patients with the same last name, the names in common are displayed in a visually distinct manner (e.g., bold, italics, different color).[13]
- Use alternate line colors for adjacent patients.[13]

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Recommended Practice

1.5 Medical record numbers incorporate a “check digit” to help prevent data entry errors.
Checklist

Implementation Status

Rationale for Practice or Risk Assessment

A “check digit” program for reducing common errors in number sequences used in patient records greatly reduces data entry errors.[23]

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- To minimize human-generated number insertion, deletion, substitution, or transposition errors or their effects, optimize processes for correct patient identification (e.g., two-person sign-off before administration of blood transfusions).
- One example of a "check digit" program is the "Verhoeff algorithm," which works with strings of decimal digits of any length and detects all single-digit errors and all transposition errors involving two adjacent digits.[24]

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Recommended Practice

1.6 Users are warned when they attempt to create a record for a new patient (or look up a patient) whose first and last names are the same as another patient, or attempt to look up a patient and the search returns multiple patients with the same or similar names.[13]
Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Using automated EHR processes to prevent duplicate records can prevent unintentional human errors that could lead to patient harm. Creating a duplicate (i.e., split) record or commingling two different patient records results in a serious patient safety risk.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- During the creation of a new patient record, a phonetic algorithm, such as Soundex, is used to display an alert or warning if the patient, or a patient with similar demographic data, exists in the system.
- When looking up a patient, if the results list returns multiple patients with similar demographic data, the names are displayed in a visually distinct manner.
- The system monitors for similar names (i.e., nicknames), or changed last names (e.g., marriage, divorce, adoption), when other demographics match.
- An alert provides additional demographic information context for the existing patient to help the user confirm or rule out that it is the same patient.

Recommended Practice

2.1 Patients are registered in a centralized, common database using standardized procedures.[14]
Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Nonstandard registration practices and lack of access to a common database are common causes of duplicate medical records on the same patient.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

Clinicians, support staff, and/or clinical administration

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- Organizational policy establishes standardized registration procedures involving the EHR and a common database to serve as the "source of truth" on whether a record already exists on a person who presents for services.
- The organization requires a picture ID[25] when verifying the identity of new patients, with appropriate alternatives for minors and others who do not have official picture IDs.
- The organization uses a picture ID, or appropriate alternative when an official picture ID is not available, or uses biometric attributes (e.g., iris or vein scan) to authenticate the identity of established patients.
- Registration clerks are trained in consistent patient entry practices across portals of entry (e.g., ER, inpatient, clinic, phone, internet).
- Registration clerks are trained to look up patients using the enterprise master patient index before creating a new record.
- When new patient records are being created during the registration process, the registrar is prompted to consider potential matches in the existing database.

Recommended Practice

2.2 The user interfaces of the training, test, and read-only backup environments of the EHR are clearly different from the production (i.e., "live") version to prevent inadvertent entry or review of patient information in the wrong system.[13]

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

If a clinician logs into and begins using the training, test, or read-only backup versions of the EHR by mistake, any information he or she attempts to enter will be lost.

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- Upon logging into a non-production environment or whenever they "sign" orders or notes, users are reminded (e.g., pop-up alert) that they are in a non-production environment (i.e., their orders will NOT be carried out).
- The screen background color on the production (i.e., "live") EHR is different from all other EHR environments to reduce the chances that a clinician will inadvertently enter orders or document their findings on a patient in a non-production (e.g., test) environment.
- EHR users are trained to understand the meaning of the visual differences between the different environments.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Recommended Practice

2.3 The organization has a process to assign a "temporary" unique patient ID (which is later merged into a permanent ID) in the event that either the patient registration system is unavailable or the patient is not able to provide the required information.[26]
Checklist

Implementation Status

Rationale for Practice or Risk Assessment

In certain cases, care needs to be delivered to patients not yet registered or where identity cannot be confirmed (e.g., those who are incapacitated). Processes must be in place to ensure that they soon have a permanent ID and to merge records to avoid duplicate or incomplete records.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- A process (automated or manual, such as naming conventions) is in place to assign temporary IDs to newborns and patients arriving at the Emergency Department unable to provide their demographic information.[27]
- Staff members are trained in areas where temporary IDs may be required (e.g., blood banking) to ensure that temporary records are integrated into permanent ones.
- Any downstream use of a temporary ID within a facility, or in transfers between facilities, is tracked and corrected in all electronic systems, including at transfer facilities.
- The organization monitors resolution of temporary IDs.

Recommended Practice

2.4 Patient identity is verified at key points or transitions in the care process (e.g., prior to procedures and surgeries, rooming patient, vital sign recording, order entry, medication administration, check out).[13]
Checklist

Implementation Status

Rationale for Practice or Risk Assessment

To avoid "wrong patient" errors, care must be taken to check the patient's identification at all critical points in the healthcare process and to ensure that EHR use is integrated into workflows that support correct patient identification.

Suggested Sources of Input

Clinicians, support staff, and/or clinical administration

Examples of Potentially Useful Practices/Scenarios

- Before opening a specific patient record or signing an order, the user is shown a picture, or the name, gender, and age of the patient.[22]
- Clinicians are asked to "re-enter" the patient's initials before signing an order.
- Workflow, including for example, use of barcodes and two-person sign-off, related to verification of patient identity is evaluated to optimize use of the EHR to prevent "wrong patient" errors.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Recommended Practice

2.5 The EHR limits the number of patient records that can be displayed on the same computer at the same time to one.[13, 28]
Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Distractions while documenting or reviewing information in the EHR are common.[18, 22] EHRs should be designed to reduce the likelihood of working with the wrong patient's record as the result of distractions. When working on multiple patients, potential gains in efficiency might be outweighed by the risks associated with entering or reviewing data on the wrong patient.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- Clinicians are engaged in developing EHR configuration and policies to prevent errors due to distractions and the resulting danger of working on the wrong patient chart when several records are open.
- Workflow is evaluated to ensure that clinicians are able to respond to urgent situations in which they may need to look at a new record without completing review of a first patient's record. The practice environment should be designed to minimize the need to open and actively use multiple patients' records on the same computer.
- Before allowing the user to change the current patient, the system checks that all entered data has been saved (i.e., signed) or deleted (e.g., the user recognizes that they are entering data on the wrong patient) before allowing the system to display a different patient's data.[29]

Recommended Practice

2.6 Patients who are deceased are clearly identified as such.
Checklist

Implementation Status

Rationale for Practice or Risk Assessment

In many instances, selection of a deceased patient represents a "wrong patient" error. Clinicians should be reminded that the patient they have selected is dead.

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- The system clearly identifies when a deceased patient's record is accessed (e.g., through a pop-up alert when opening the record or a different background color for the deceased patient header in the EHR).

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Recommended Practice

2.7 The use of test patients in the production (i.e., "live") environment is carefully monitored. When they do exist, they have unambiguously assigned "test" names (e.g., including numbers or multiple Z's) and are clearly identifiable as test patients (e.g., different background color for patient header).[13, 30]
Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Test patients in the production system are necessary to facilitate end-to-end testing, but care must be taken to ensure that they are not mistaken for real patients.

Suggested Sources of Input

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- Test patients should have names that clearly identify them as such: BWH17, ZZZOrders or MGH23zz, ZResults (examples are last name, first name).
- "Cute" names (e.g., Marcus Welby, Jim Test) should not be used as test patients as there could be real patients with those names.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Recommended Practice

3.1 The organization regularly monitors its patient database for patient identification errors and potential duplicate patients or records.[11, 14, 16, 31, 32]

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Avoidable patient identification errors are a risk both to patients and to the organization. Monitoring reduces the likelihood that patients will be misidentified and harmed as a result.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- The organization has a policy to periodically monitor its EHR database for common scenarios related to wrong patient identification (e.g., changes in patient blood type over time).
- The NQF-endorsed "order–retract–reorder" algorithm can be used to measure the rate of erroneous orders due to patient ID errors (NQF #2723: Wrong Patient Retract and Reorder [WP-RAR]).[16, 22]
- The “inconsistent gender algorithm” (e.g., use of female pronouns in progress note of male patient) can be used to estimate the number of erroneous freetext notes due to patient ID errors.[31]
- The EHR has a mechanism to run a report listing potential duplicate patient records (e.g., records that contain virtually the same clinical and demographic information for patients with different names).
- Once identified through monitoring, duplicate records are detected and merged.[14, 16]
- Industry standards for duplicate record error rates are available. The organization consistently monitors its own duplicate record error rate, and ensures that it remains at or below industry standards.[11, 14, 16, 32]

References

1. Kowalczyk, L. (2013, March 7). Brigham and Women's Hospital video uses slapstick to promote patient safety. Retrieved August 8, 2016, from Boston.com.

2. Bittle, M. J., Charache, P., & Wassilchalk, D. M. (2007). Performance improvement: registration-associated patient misidentification in an academic medical center: causes and corrections. The Joint Commission Journal on Quality and Patient Safety, 33(1), 25-33.

3. DuVall, S. L., Kerber, R. A., & Thomas, A. (2010). Extending the Fellegi–Sunter probabilistic record linkage method for approximate field comparators. Journal of Biomedical Informatics, 43(1), 24-30.

4. Miller, P. L., Frawley, S. J., & Sayward, F. G. (2001). Exploring the utility of demographic data and vaccination history data in the deduplication of immunization registry patient records. Journal of Biomedical Informatics, 34(1), 37-50.

5. Lee, A. C., Leung, M., & So, K. T. (2005). Managing patients with identical names in the same ward. International Journal of Health Care Quality Assurance, 18(1), 15-23.

6. Arellano, M. G., & Weber, G. I. (1998). Issues in identification and linkage of patient records across an integrated delivery system. Journal of Healthcare Information Management, 12(3), 43-52.

7. Henneman, P. L., Fisher, D. L., Henneman, E. A., Pham, T. A., Campbell, M. M., & Nathanson, B. H. (2010). Patient identification errors are common in a simulated setting. Annals of Emergency Medicine, 55(6), 503-509.

8. O'Neill, K. A., Shinn, D., Starr, K. T., & Kelley, J. (2004). Patient misidentification in a pediatric emergency department: patient safety and legal perspectives. Pediatric Emergency Care, 20(7), 487-492.

9. Ranger, C. A., & Bothwell, S. (2004). Making sure the right patient gets the right care. Quality and Safety in Health Care, 13(5), 329-329.

10. Sideli, R. V., & Friedman, C. (1991). Validating patient names in an integrated clinical information system. Proceedings of the Annual Symposium on Computer Application in Medical Care (p. 588). American Medical Informatics Association.

11. McCoy, A. B., Wright, A., Kahn, M. G., Shapiro, J. S., Bernstam, E. V., & Sittig, D. F. (2013). Matching identifiers in electronic health records: implications for duplicate records and patient safety. BMJ Quality & Safety, 22(3), 219-224.

12. American Health Information Management Association. Reconciling and managing EMPIs (Updated). (2010). Journal of the American Health Information Management Association, 81(4), 52-57.

13. Lowry, S. Z., Quinn, M. T., Ramaiah, M., Schumacher, R. M., Patterson, E. S., North, R., ... & Abbott, P. (2012). Technical evaluation, testing, and validation of the usability of electronic health records. National Institute of Standards and Technology.

14. Dooling, J. A., Durkin, S., Fernandes, L., Just, B., Kotyk, S., Karl, E. S., & Westhafer, K. (2014). Managing the integrity of patient identity in health information exchange (updated). Journal of the American Health Information Management Association, 85(5), 60.

15. Smith, J.A. (2010). Fundamentals for building a master patient index/enterprise master patient index. Journal of the American Health Information Management Association.

16. Identification and prioritization of health IT patient safety measures. (February, 2016). National Quality Forum.

17. Understanding file permissions on Unix: a brief tutorial. (n.d.). Darthmouth.

18. Mardon, R., Olinger, L., Szekendi, M. (2014). Health information technology adverse event reporting: analysis of two databases. ECRI, Westat, UHC, editors. Office of the National Coordinator for Health Information Technology.

19. National patient safety goals effective January 1, 2016. (2016). The Joint Commission.

20. Valenstein, P. N., & Sirota, R. L. (2004). Identification errors in pathology and laboratory medicine. Clinics in Laboratory Medicine, 24(4), 979-996.

21. NHS CUI design guide workstream design guide entry - patient banner version 4.0.0.0 baseline. (2015). Health & Social Care Information Centre.

22. Adelman, J. S., Kalkut, G. E., Schechter, C. B., Weiss, J. M., Berger, M. A., Reissman, S. H., ... & Southern, W. N. (2013). Understanding and preventing wrong-patient electronic orders: a randomized controlled trial. Journal of the American Medical Informatics Association, 20(2), 305-310.

23. Kirtland, J. (2001). Identification numbers and check digit schemes. The Mathematical Association of America.

24. Salomon, D. (2006). Coding for data and computer communications. Springer Science & Business Media.

25. Hyman, D., Laire, M., Redmond, D., & Kaplan, D. W. (2012). The use of patient pictures and verification screens to reduce computerized provider order entry errors. Pediatrics, 130(1), e211-e219.

References

26. Sittig, D. F., Ash, J. S., Zhang, J., Osheroff, J. A., & Shabot, M. M. (2006). Lessons from "Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system." Pediatrics, 118(2), 797-801.

27. Adelman, J., Aschner, J., Schechter, C., Angert, R., Weiss, J., Rai, A., ... & Racine, A. (2015). Use of temporary names for newborns and associated risks. Pediatrics, 136(2), 327-333.

28. Paparella, S. F. (2012). Accurate patient identification in the emergency department: meeting the safety challenges. Journal of Emergency Nursing, 38(4), 364-367.

29. Sittig, D. F., Teich, J. M., Yungton, J. A., & Chueh, H. C. (1997). Preserving context in a multi-tasking clinical environment: a pilot implementation. Proceedings of the AMIA Annual Fall Symposium (p. 784). American Medical Informatics Association.

30. Wright, A., Aaron, S., & Sittig, D. F. (2016). Testing electronic health records in the "production" environment: an essential step in the journey to a safe and effective health care system. Journal of the American Medical Informatics Association.

31. Wilcox, A. B., Chen, Y. H., & Hripcsak, G. (2011). Minimizing electronic health record patient-note mismatches. Journal of the American Medical Informatics Association, 18(4), 511-514.

32. Zech, J., Husk, G., Moore, T., & Shapiro, J. S. (2016). Measuring the degree of unmatched patient records in a health information exchange using exact matching. Applied Clinical Informatics, 7(2), 330-340.