Self Assessment

System Interfaces

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 (2013), 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, clinical practice standards, regulations and policy, and associated industry practices 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.

In some instances, Meaningful Use and/or HIPAA Security Rule requirements are identified in connection with recommended practices. The SAFER Guides are not intended to be used for legal compliance purposes, and implementation of a recommended practice does not guarantee compliance with Meaningful Use, HIPAA, or other laws. 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 or offer recommendations based on a healthcare provider's specific circumstances. Users of the SAFER Guides are encouraged to consult with their own legal counsel with regard to compliance with Meaningful Use, HIPAA, and other laws. For more information on Meaningful Use, 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

System Interfaces

Introduction

The *System Interfaces SAFER Guide* identifies recommended safety practices intended to optimize the safety and safe use of system-to-system interfaces between EHR-related software applications. Many healthcare organizations are involved in planning, implementing, or maintaining enterprise- or community-wide clinical information systems that require integration.[1] Such integration occurs most often via interfaces between software applications, often from different system developers. These interfaces send and receive information, enabling disparate systems to operate on the same data.

System interface projects are complex because they involve many stakeholders (e.g., clinicians, administrators, and information technologists) in various departments, often with differing agendas. Stakeholders must work with hardware devices and software applications that are developed independently, while integrating them flawlessly with complex clinical work processes. Well-designed and well-developed system interfaces enable reliable physical and logical connection of different systems. System interfaces require physical equipment (e.g., hardware such as plugs, cables, and cards), software that controls the data and information that is exchanged, and concepts (e.g., data protocols and controlled vocabularies) that control the interactions between systems. In addition to these technical issues, interfaces involve social and organizational factors, such as agreements to provide data in a consistent format and to use data to refer to concepts in a consistent manner (i.e., multiple systems must manage and coordinate any change to the meaning of a data item). Processes and preparations must be in place to ensure appropriate configuration and maintenance of interfaces.[2] For example, a mapping error between the order entry system and the pharmacy can cause dispensing of the wrong drug.[3] Similarly, researchers have identified errors in the transmission of free-text comment fields between the order entry application and the pharmacy system.[4]

Completing the self-assessment in the *System Interfaces SAFER Guide* requires the engagement of people both within and outside the organization (such as EHR technology developers). Because this guide is designed to help organizations prioritize interface-related safety concerns, including the meaning of the data in the EHR, 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 system interface 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 interface-related safety risks introduced by the EHR.

Self Assessment

System Interfaces

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 *Phase* associated with the *Recommended Practice(s)* appears at the top of the column. Click on the link to access more information about the Phases and Principles from the website.

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

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

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
1	Hardware that runs applications critical to the organization's operation is duplicated.	Worksheet 1	○	○	○	reset
2	An electric generator and sufficient fuel are available to support the EHR during an extended power outage.	Worksheet 2	○	○	○	reset
3	Paper forms are available to replace key EHR functions during downtimes.	Worksheet 3	○	○	○	reset
4	Patient data and software application configurations critical to the organization's operations are backed up.	Worksheet 4	○	○	○	reset
5	Policies and procedures are in place to ensure accurate patient identification when preparing for, during, and after downtimes.	Worksheet 5	○	○	○	reset

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

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
6	Staff are trained and tested on downtime and recovery procedures.	Worksheet 6	○	○	○	reset
7	A communication strategy that does not rely on the computing infrastructure exists for downtime and recovery periods.	Worksheet 7	○	○	○	reset
8	Written policies and procedures on EHR down-times and recovery processes ensure continuity of operations with regard to safe patient care and critical business operations.	Worksheet 8	○	○	○	reset
9	The user interface of the locally maintained backup, read-only EHR system is clearly differentiated from the live/production EHR system.	Worksheet 9	○	○	○	reset

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

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
10	There is a comprehensive testing and monitoring strategy in place to prevent and manage EHR down-time events.	Worksheet 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 **Phase 1 — Safe Health IT***

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
1	The EHR supports and uses standardized protocols for exchanging data with other systems.	*Worksheet 1*	○	○	○	reset
2	Established and up-to-date versions of operating systems, virus and malware protection software, application software, and interface protocols are used.	*Worksheet 2*	○	○	○	reset
3	System-to-system interfaces support the standard clinical vocabularies used by the connected applications.	*Worksheet 3*	○	○	○	reset
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 4*	○	○	○	reset
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 5*	○	○	○	reset
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 6*	○	○	○	reset
7	Changes to hardware or software on either side of the interface are tested before and monitored after go-live.	*Worksheet 7*	○	○	○	reset
8	There is a hardware and software environment for interface testing that is physically separate from the live environment.	*Worksheet 8*	○	○	○	reset
9	Policies and procedures describe how to stop and restart the exchange of data across the interface in an orderly manner.	*Worksheet 9*	○	○	○	reset
10	Security procedures, including role-based access, are established for managing and monitoring key designated aspects of interfaces and data exchange.	*Worksheet 10*	○	○	○	reset

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

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
11	The organization has access to personnel with the skills required to configure, test, and manage all operational system-to-system interfaces.	*Worksheet 11*	○	○	○	reset
12	Administrative, financial, and clinical data exchange needs are clearly documented and include how data will be used and who is responsible for maintaining the interface and the systems connected to it.	*Worksheet 12*	○	○	○	reset
13	The organization notifies people involved in maintenance or use of system interfaces when changes are made that affect the content of the standard data files or allowable values transmitted via the interface (e.g., the orderable catalog or charge master).	*Worksheet 13*	○	○	○	reset
14	The operational status of the system interface is clear to its users with regard to clinical use, such as knowing when the interface cannot transmit or receive messages, alerts, or crucial information.	*Worksheet 14*	○	○	○	reset
15	The interface is able to transmit contextual information, such as units for measures or sources of information, to enable clinicians to properly interpret information.	*Worksheet 15*	○	○	○	reset
16	Interface problems associated with known system interface risks and data field size limits are managed to avoid readily preventable errors.	*Worksheet 16*	○	○	○	reset

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

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
17	The organization monitors the performance and use of system interfaces regularly, including monitoring the interface error log and the volume of transactions over the interface.	*Worksheet 17*	○	○	○	reset
18	When interface errors are detected, they are reported, fixed, and used to construct new test cases to improve the interface testing.	*Worksheet 18*	○	○	○	reset

A multidisciplinary 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

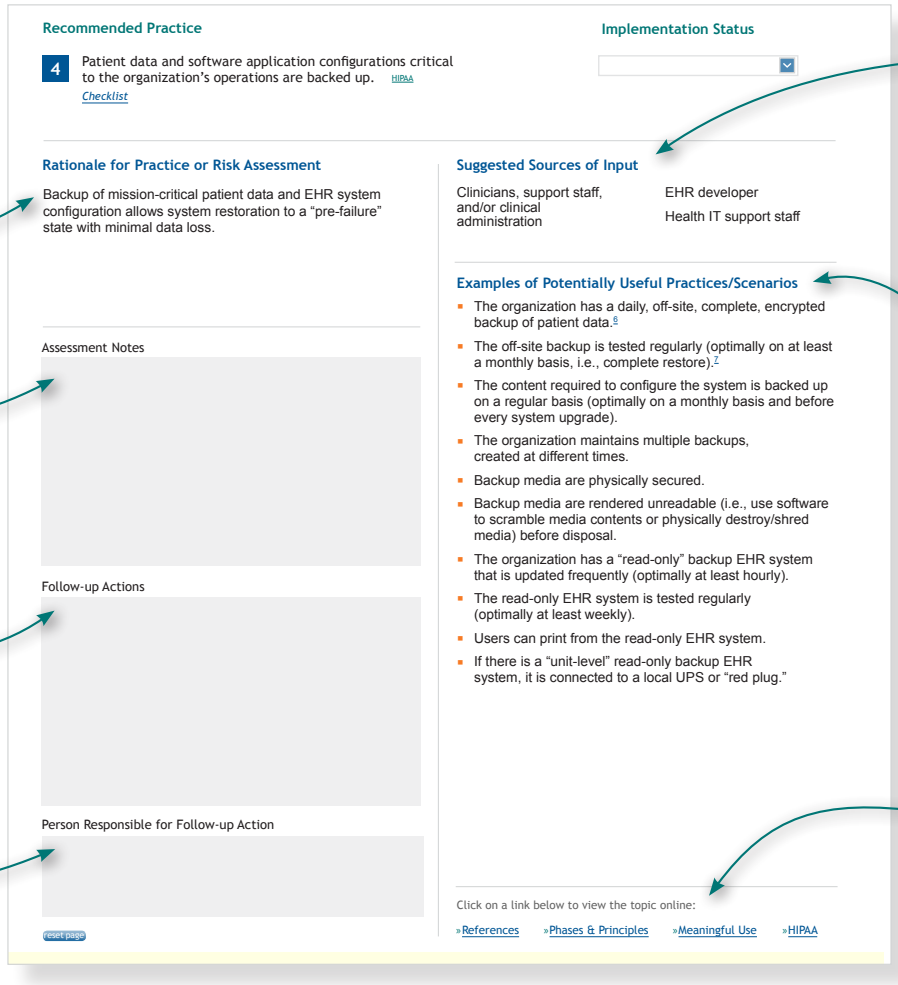
Each *Worksheet* provides guidance on implementing a specific *Recommended Practice*, and allows you to enter and print information about your self-assessment.

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*.

Each *Worksheet* shows links to additional information available on the website.

Recommended Practice

1 The EHR supports and uses standardized protocols for exchanging data with other systems.[5]

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Standards, such as those developed by HL7, greatly simplify the establishment and maintenance of safe and effective interfaces between EHRs and external systems (e.g., ancillaries such as laboratory, radiology, or pharmacy), thereby reducing communication errors.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

- Clinicians, support staff, and/or clinical administration
- Diagnostic services
- EHR developer
- Health IT support staff
- Pharmacy

Examples of Potentially Useful Practices/Scenarios

- At a minimum, the EHR satisfies ONC's certification requirements related to electronic exchange of information.
- The EHR is capable of sending and receiving clinical and administrative data using HL7 version 2.x messages where the sending and receiving systems use the same version.
- The EHR has 2-way, HL7 v 2.x-compatible interfaces to mission critical ancillary systems (at a minimum: pharmacy, laboratory, blood bank, and radiology).
- The EHR is capable of generating, exporting, importing, and decoding clinical patient summary documents encoded in the Continuity of Care Document (CCD) standard.[6] This includes procedures such as placing the correctly decoded clinical data into the proper location in the EHR, rather than just adding a human-readable version of the document to the patient's list of free text reports.
- If the organization has an "interface engine," the hardware running this application is duplicated (i.e., operational backup hardware is installed).[7]
- Both the sending and receiving side of the interfaces are documented in sufficient detail to allow both sides to validate the adequacy of the interface for use.[8]
- The EHR has links to external clinical information reference resources using the HL7 InfoButton standard.[9]
- When sending data across the Internet or other public networks, the EHR uses a secure, encrypted, transmission protocol (e.g., SSL - Secure Sockets Layer or TSL - Transport Layer Security) to ensure the data's security while in transit (e.g., when sending a prescription to an outside pharmacy via Surescripts).

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

2 Established and up-to-date versions of operating systems, virus and malware protection software, application software, and interface protocols are used. HIPAA

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Failure to stay up-to-date with the latest versions of software and interface protocols places the organization at risk of clinical and administrative data loss, corruption, or theft.

Suggested Sources of Input

- Diagnostic services
- EHR developer
- Health IT support staff
- Pharmacy

Examples of Potentially Useful Practices/Scenarios

- The organization has policies and procedures to determine how soon version testing and implementation will occur after the release of new software.
- The organization has employees or service providers responsible for monitoring and upgrading software and communication protocols as needed.
- Operating systems, virus and malware protection software, application software, and interface protocols in use are supported by their suppliers.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

3 System-to-system interfaces support the standard clinical vocabularies used by the connected applications.

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Use of standard clinical vocabularies is essential to ensure semantic interoperability (i.e., consistent interpretation of the meaning of terms) between systems.

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 interface supports and encourages use of clinical vocabularies from ONC's certification requirements, for example: RxNorm for medication names,[10] SNOMED-CT for clinical problems,[11] and LOINC for laboratory tests.[12]
- A process is in place to ensure that standard clinical vocabularies are updated and consistent in all interfaced software applications.
- Organizations evaluate interfaced software prior to purchase to ensure that it uses compatible versions of standard clinical vocabularies.

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

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. HIPAA

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Maintaining a system-to-system interface within a rapidly evolving clinical information system environment is challenging, in part because many changes are required. Without the ability to implement and test these changes prior to go-live, and a consistent practice of doing so, patients would be placed at significantly increased risk of data loss, corruption, or theft. Failure to test system interface components is one of the leading causes of EHR-related patient safety events.[13]

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

- System-to-system interfaces are tested before going into production and after changes to hardware, software, or content (e.g., the allowable list of data elements to be exchanged) on either side of the interface.
- Free text data fields accessible to clinical end users of one system are transferred intact (i.e., no changes or truncation of characters) to the other system.
- The organization (or interface developer) should develop a reference or validation data set that includes boundary cases (i.e., data that are slightly below, at, and slightly above key thresholds). These test data are run through the interface repeatedly after any change to the hardware or software on either end of the interface to document that the interface is continuing to work appropriately.

Click on a link below to view the topic online:

» References » Phases & Principles » HIPAA

Recommended Practice

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.[14] HIPAA

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

While ideally everything should be carefully tested, the demands of testing must also be reasonable. The more important the data is to patient safety, the more interface testing should be conducted.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

- Clinicians, support staff, and/or clinical administration
- Diagnostic services
- EHR developer
- Health IT support staff
- Pharmacy

Examples of Potentially Useful Practices/Scenarios

- When testing an interface, both anticipated and unanticipated types of data (e.g., text characters in a numeric field) and amounts of data should be used to ensure that the interface does not respond incorrectly in either case.
- Organizations, through policies and/or job descriptions, address responsibility for evaluation of the intensity and extent of interface testing for all new software purchases or upgrades of systems that must be interfaced.
- Organizations address the role of EHR technology developers in the testing of interfaces, and incorporate expectations in contractual and service obligations.

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

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.[15] HIPAA

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

At the time of major system changes, social factors can interact with technical factors to create new risks. Information, even when correctly encoded and transmitted, can be misinterpreted because of differences in how users conceptualize their work.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

- Clinicians, support staff, and/or clinical administration
- Diagnostic services
- EHR developer
- Health IT support staff
- Pharmacy

Examples of Potentially Useful Practices/Scenarios

- Testing uses a wide range of cases and scenarios including those where users of the external application or users in the external facility or service may interpret things differently (e.g., “day” may mean different things to a 24/7 facility and a 9-5 facility; and “home phone” means different things to a college campus clinic, a nursing home, an urban “safety net” community clinic, and a private physician practice).
- When a new system is connected or integrated, testing includes looking for ways that correctly transmitted and coded information could nevertheless be misinterpreted. For example, in the first few weeks of using a newly integrated system, staff is designated to observe use of the software or to talk to users (in person or by phone) to confirm the receipt and intended interpretation and use of information and messages sent via the interface.[16]
- Testing should include real-world, clinical scenarios of information exchange, such as: schedule an appointment; admit a patient; place an order; process order in ancillary lab; report results; record medication administration.

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

7 Changes to hardware or software on either side of the interface are tested before and monitored after go-live. HIPAA

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Hardware and software updates are inevitable. If the new hardware or software is unable to handle the load of transactions or otherwise work as intended in the actual workplace, it may shut down or compromise data integrity.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

- Diagnostic services
- EHR developer
- Health IT support staff
- Pharmacy

Examples of Potentially Useful Practices/Scenarios

- Upgrades to EHR and ancillary systems are supported by additional testing of the system-to-system interfaces involved.
- The organization carries out "load testing" (e.g., run a large number of transactions through the interface in a short period of time), and "stress testing" (e.g., send erroneous random data through the interface to potentially induce unexpected outputs) to ensure that the system can handle the required load at peak times and when confronted with erroneous data.[17]

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

8 There is a hardware and software environment for interface testing that is physically separate from the live environment.

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

EHRs and the many applications they must interface with are continually changing. System administrators and application developers need a "safe" place to develop and test these changes without fear of causing harm to patients.

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- Changes to applications (or the content to be exchanged) on either side of the interface, or to the interface itself, are implemented and tested in the test/development environment before being put into production.
- Develop and test batch processing jobs for applications and interfaces.
- Regression testing (i.e., to ensure that all previous functionality is still working appropriately) is conducted in the test environment before changes are promoted to the production system.[18]

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

9 Policies and procedures describe how to stop and restart the exchange of data across the interface in an orderly manner.

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Failure to stop and restart an interface properly can result in "in transit" data being lost or corrupted without any warning to users.

Suggested Sources of Input

- Diagnostic services
- EHR developer
- Health IT support staff
- Pharmacy

Examples of Potentially Useful Practices/Scenarios

- Ensure that all system interface buffers are empty prior to stopping or restarting the system.
- If the interface must be disconnected while the sending system continues to produce data for transmission, e.g., lab tests ordered through CPOE, the buffers are of adequate size and behavior to prevent any loss of data.
- The organization has a method of communicating to users when a clinical interface is not functioning properly (e.g., an alert on the login page, or a user-appropriate alert in the EHR whenever data retrieval or transmission is attempted but not completed).
- Ensure reliable procedures are in place and used for stopping and starting system interfaces. The procedures are available and consulted during hardware/software upgrades.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Click on a link below to view the topic online:

» References » Phases & Principles » HIPAA

Recommended Practice

10 Security procedures, including role-based access, are established for managing and monitoring key designated aspects of interfaces and data exchange.[19] HIPAA

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

The integrity and confidentiality of data within applications must be well-protected. When data moves between systems there is an increased risk of data loss, corruption, or theft. Both physical and logical security controls are required over this exchange of data to prevent unintended changes.

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 server hosting the interface hardware and software is maintained in a physically secure (i.e., locked room) location.
- The server hosting the "interface engine" has a secure administrator login to prevent unauthorized changes to the interface configuration or access to the data as it crosses the interface.
- System security is tested to ensure that unauthorized individuals or applications cannot alter or gain access to protected health information.
- The security procedures identify and protect key designated aspects of the interfaces, including content mapping applications,[19] the content maps themselves, error logs, and clinical data.

Click on a link below to view the topic online:

» References » Phases & Principles » HIPAA

Recommended Practice

11 The organization has access to personnel with the skills required to configure, test, and manage all operational system-to-system interfaces.

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Configuring, testing, and managing system-to-system interfaces are complex tasks. The organization must ensure that only certified or qualified personnel are assigned to configure, test, and manage the system prior to go-live.

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- Help desk operator manuals for quick reference are developed, readily available, and up-to-date.
- Assigned personnel are trained on all system-to-system interface maintenance and monitoring activities, or have appropriate access to qualified personnel.
- The organization identifies who is able to access help from the EHR developer and other external experts.
- The organization has a plan for getting access to key individuals during off-hours (i.e., after routine business hours and on weekends and holidays).
- Training or certification of personnel assigned to configure, test, and manage interfaces is reviewed on a regular basis, at least annually, to ensure staff is adequately trained and afforded the opportunity to update training.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

12 Administrative, financial, and clinical data exchange needs are clearly documented and include how data will be used and who is responsible for maintaining the interface and the systems connected to it.[20] HIPAA

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Failure to document the business needs and responsibilities for the interface can result in miscommunication regarding the meaning and timing of the exchange of information and lead to patient harm.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

- Diagnostic services
- EHR developer
- Health IT support staff
- Pharmacy

Examples of Potentially Useful Practices/Scenarios

- All types of data to be exchanged via the interface are clearly specified including: allowable values (e.g., text vs. numeric, length or size of fields, etc.); clinical vocabularies used; and how associated values (i.e., metadata) will be communicated (e.g., representation of units on measurements, sources of data, etc.).
- The interface is designed to handle the estimated mean and maximum amounts of data expected to cross the interface with acceptable performance and errors generated.
- The organization maintains a comprehensive data dictionary that includes, for each data element:
  - Data type (e.g., coded, text, numeric)
  - Data definition
  - Metadata – (e.g., creator, date created, users)
- The organization maintains a comprehensive interface data map that includes data recodes or conversions, as required.
- The organization maintains a set of interface system performance requirements including the expected throughput of the system, uptime requirements, and protocols supported.

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

13 The organization notifies people involved in maintenance or use of system interfaces when changes are made that affect the content of the standard data files or allowable values transmitted via the interface (e.g., the orderable catalog or charge master). HIPAA

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

EHR-related hardware and software change frequently. Failure to notify all parties involved in the maintenance or use of the system interfaces often results in interface errors. Some of these errors may be subtle and difficult to identify. Failure to account for and manage the changes can lead to serious patient safety events.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

- Diagnostic services
- EHR developer
- Health IT support staff
- Pharmacy

Examples of Potentially Useful Practices/Scenarios

- Changes are clearly communicated and tested prior to go-live, including changes to: conversion programs, interfaces, databases, screens (e.g., length of data entry or display fields), tables (e.g., data interpretation, numeric values, times, dates, or text-based data fields), and vocabularies.
- Documentation that appropriate testing has occurred after all system modifications is available.
- There is a policy describing configuration control procedures that includes: who must be notified before any change is made, who can make the changes, who is responsible for testing the changes, who is responsible for approving the changes, and when the changes can be implemented in the live system.

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

14 The operational status of the system interface is clear to its users with regard to clinical use, such as knowing when the interface cannot transmit or receive messages, alerts, or crucial information. HIPAA

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Users must be notified when the interface between clinical systems is not functioning properly. Failure to distinguish between "there are no results" and "the interface to the system containing the results is not functioning" could lead to diagnostic or therapeutic delays.

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- The user is informed when the interface cannot transmit a message.
- The user is informed when the remote system from which they are requesting information is unavailable, due to errors in the interface or the remote system itself.
- The user is notified when drug-allergy testing is performed on local medications only, excluding those identified by remote pharmacies or health information exchanges.
- EHR applications that depend on system interfaces should report the interface status when in use (e.g., while reviewing imaging studies, the EHR shows the last update time or current connection with the PACS system).

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

15 The interface is able to transmit contextual information, such as units for measures or sources of information, to enable clinicians to properly interpret information.

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Failure to transmit the relevant metadata (i.e., context or details) related to the data, and necessary for its interpretation, can lead to misunderstandings and erroneous decisions.

Suggested Sources of Input

- Diagnostic services
- EHR developer
- Health IT support staff
- Pharmacy

Examples of Potentially Useful Practices/Scenarios

- The interface can transmit the units for measurements along with the measurements, and the units are stored in structured data fields (e.g., 175 *lbs.* or 500 *mg*).
- The interface can transmit information associated with a particular measure (e.g., fraction of inspired oxygen accompanies the arterial blood gas results to allow clinicians to interpret the blood gas values in the proper context).

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

16 Interface problems associated with known system interface risks and data field size limits are managed to avoid readily preventable errors.[21] HIPAA

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Physical and logical interfaces have limitations. Failure to acknowledge and plan for these limitations often results in patient safety events.

Suggested Sources of Input

- Diagnostic services
- EHR developer
- Health IT support staff
- Pharmacy

Examples of Potentially Useful Practices/Scenarios

- The sending system identifies and restricts messages that are not transmittable (e.g., incorrect data type).
- The user is notified if what he or she is typing exceeds the maximum size for either the storage location or the system-to-system interface.[22]
- The organization has a process for managing and minimizing known risks associated with interface problems, such as two systems with different field size limits. The system with the smaller limit can cause data to be truncated unless the risk is addressed properly.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

17 The organization monitors the performance and use of system interfaces regularly, including monitoring the interface error log and the volume of transactions over the interface.[24] HIPAA

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

System-to-system interfaces are complex and many of their actions are not directly visible. Extensive system monitoring is required to help identify and track hidden errors before they affect patients.

Suggested Sources of Input

- Diagnostic services
- EHR developer
- Health IT support staff
- Pharmacy

Examples of Potentially Useful Practices/Scenarios

- The system-to-system interface error log is automatically monitored and all failed transactions are brought to the attention of the appropriate staff member, investigated, and fixed within one week.[23]
- The number of transactions crossing the interface is monitored to ensure that the number of transactions is "normal" (e.g., displayed in a control chart showing the mean and reasonable upper and lower bounds, such as, 2 or 3 standard deviations from the mean).

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

18 When interface errors are detected, they are reported, fixed, and used to construct new test cases to improve the interface testing. HIPAA

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Failure to fix interface errors in a timely manner can lead to patient harm or to loss of clinicians' confidence in the data.

Suggested Sources of Input

- Diagnostic services
- EHR developer
- Health IT support staff
- Pharmacy

Examples of Potentially Useful Practices/Scenarios

- After any interface error is detected and fixed, additional tests are added to the standard set of tests to check for the same error in future releases.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA