Self-Assessment

Contingency Planning

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

Contingency Planning

Introduction

The *Contingency Planning SAFER Guide* identifies recommended safety practices associated with planned or unplanned EHR unavailability—instances in which clinicians or other end users cannot access all or part of the EHR. Occasional temporary unavailability of EHRs is inevitable, due to failures of software and hardware infrastructure, as well as power outages and natural and man-made disasters. Such unavailability can introduce substantial safety risks to organizations that have not adequately prepared. Effective contingency planning addresses the causes and consequences of EHR unavailability, and involves processes and preparations that can minimize the frequency and impact of such events, ensuring continuity of care.

EHR unavailability, which will occur in every EHR-enabled healthcare environment,[1] represents a significant potential patient safety hazard that directly affects patient care. Documented potential hazards include an increased risk of medication errors,[2] unavailability of images,[3] and canceled procedures. The potential impact of EHR unavailability increases as such systems are deployed across multiple, geographically dispersed facilities within a healthcare system.[4] The contingency planning team should include practicing clinicians to ensure that the technical components align with and support the clinical processes and workflows impacted by their decisions. The substitute workflows that must be designed and then employed during downtimes are particularly sensitive to clinician input and cooperation. In addition to the substantial initial contingency planning effort, a continuous, reliable review and maintenance process must be developed and followed. EHR safety and effectiveness can be improved by establishing proper downtime procedures, policies, and practices. The collaboration between clinicians and staff members in completing the self-assessment in this guide will enable an accurate snapshot of the organization's EHR contingency planning 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.

Interaction with HIPAA

While this guide focuses on patient safety, many of its recommendations overlap with standards and implementation specifications of the HIPAA Security Rule, which focuses on ensuring the confidentiality, integrity, and availability of electronic protected health information. Because the focus of the guide differs from that of the Security Rule, completing the checklist here will not equate with compliance with HIPAA. However, creating a contingency plan as required by the HIPAA Security Rule will address many, but not all, of the recommended safety-oriented practices in this guide. We encourage coordination of completion of the self-assessment in this SAFER Guide with contingency planning for purposes of HIPAA compliance to provide a uniform approach to patient safety and data protection.

Self-Assessment

Contingency Planning

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.

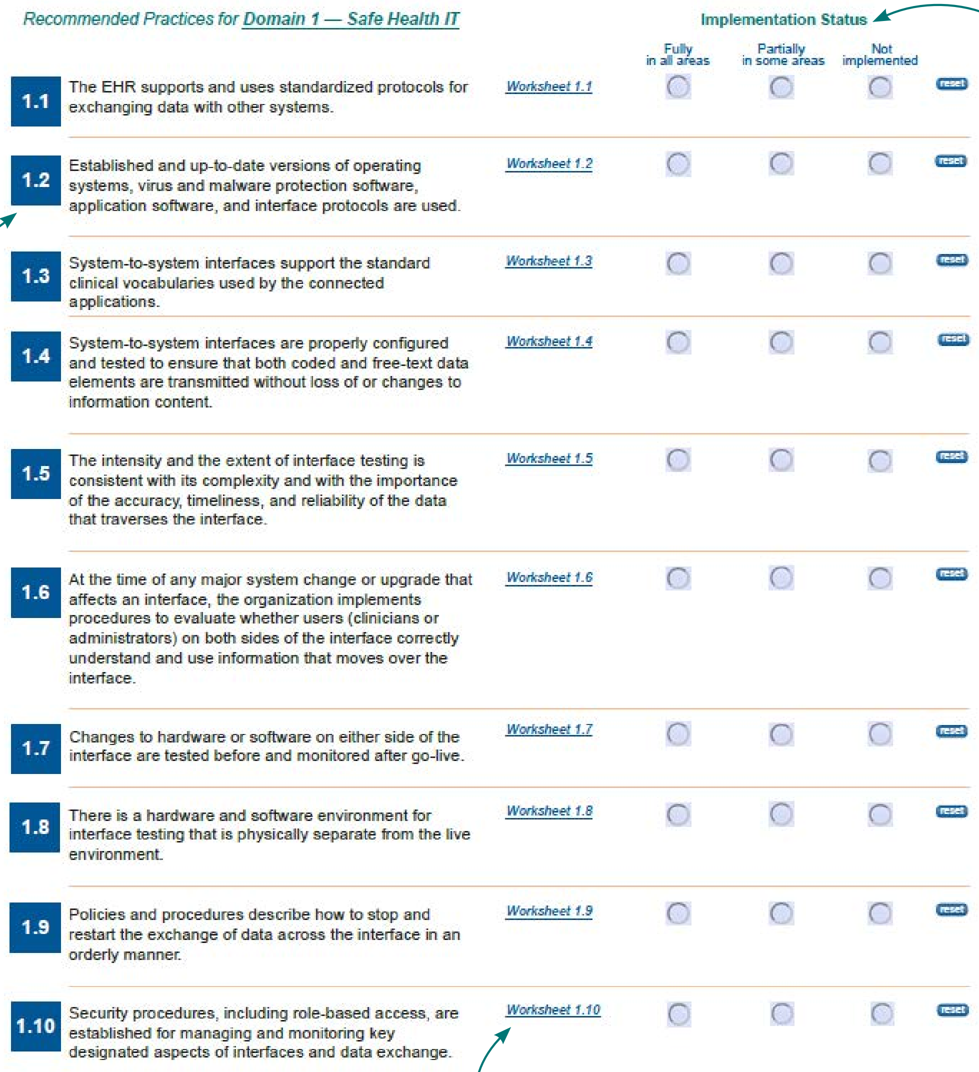
The contents of the publication or project are solely the responsibility of the authors and do not necessarily represent the official views of the U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology.

About the Checklist

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	Hardware that runs applications critical to the organization's operation is duplicated.	*Worksheet 1.1*	○	○	○	reset
1.2	An electric generator and sufficient fuel are available to support the EHR during an extended power outage.	*Worksheet 1.2*	○	○	○	reset
1.3	Paper forms are available to replace key EHR functions during downtimes.	*Worksheet 1.3*	○	○	○	reset
1.4	Patient data and software application configurations critical to the organization's operations are backed up.	*Worksheet 1.4*	○	○	○	reset
1.5	Policies and procedures are in place to ensure accurate patient identification when preparing for, during, and after downtimes.	*Worksheet 1.5*	○	○	○	reset

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

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
2.1	Staff are trained and tested on downtime and recovery procedures.	*Worksheet 2.1*	○	○	○	reset
2.2	A communication strategy that does not rely on the computing infrastructure exists for downtime and recovery periods.	*Worksheet 2.2*	○	○	○	reset
2.3	Written policies and procedures on EHR downtimes and recovery processes ensure continuity of operations with regard to safe patient care and critical business operations.	*Worksheet 2.3*	○	○	○	reset
2.4	The user interface of the locally maintained backup, read-only EHR system is clearly differentiated from the live/production EHR system.	*Worksheet 2.4*	○	○	○	reset
2.5	Users are trained on ransomware prevention strategies including how to identify malicious emails.	*Worksheet 2.5*	○	○	○	reset

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

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
3.1	There is a comprehensive testing and monitoring strategy in place to prevent and manage EHR downtime events.	*Worksheet 3.1*	○	○	○	reset
3.2	Functional system downtimes (i.e., unacceptably slow response time) are identified and addressed proactively.	*Worksheet 3.2*	○	○	○	reset
3.3	Review unexpected extended system downtimes greater than 24 hours using root-cause analysis or similar approaches.	*Worksheet 3.3*	○	○	○	reset

Team Worksheet

>Table of Contents | >About the Checklist | >Team Worksheet | >About the Practice Worksheets | >Practice Worksheets

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

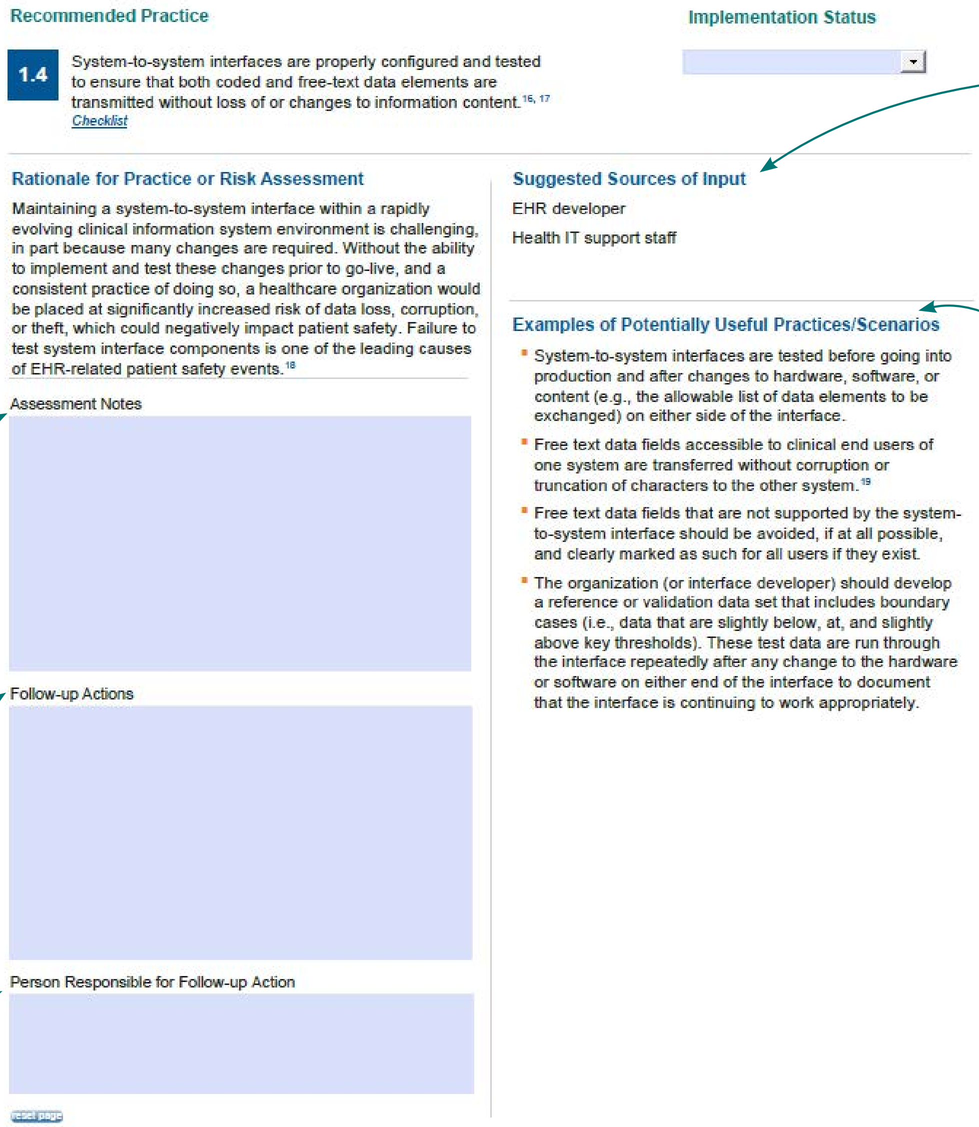
Assessment Completion Date

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.



Recommended Practice

Implementation Status

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.[16, 17]
Checklist

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, a healthcare organization would be placed at significantly increased risk of data loss, corruption, or theft, which could negatively impact patient safety. Failure to test system interface components is one of the leading causes of EHR-related patient safety events.[18]

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

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 without corruption or truncation of characters to the other system.[19]
- Free text data fields that are not supported by the system-to-system interface should be avoided, if at all possible, and clearly marked as such for all users if they exist.
- 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.

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 Hardware that runs applications critical to the organization's operation is duplicated.
Checklist

Implementation Status

Off

Rationale for Practice or Risk Assessment

Organizations should take steps to prevent and minimize the impact of technology failures. A single point of failure greatly increases risks both for the availability and integrity of data.

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

- A large healthcare organization that provides care 24 hours per day has a remotely located (i.e., > 50 miles away and > 20 miles from the coastline) "warm-site" (i.e., a site with current patient data that can be activated in less than 8 hours) backup facility that can run the entire EHR.[5]
- The warm-site is tested at least quarterly.
- The organization maintains a redundant path to the Internet consisting of two different cables, in different trenches (a microwave or other form of wireless connection is also acceptable), provided by two different Internet providers.[6, 7]
- Smaller ambulatory clinics have at least a cellphone-based, wireless Internet access point as a backup to their main cable-based Internet connection.
- If using a remotely hosted EHR (e.g., cloud-based solution), insist that your EHR provider back up data with tape, Internet, redundant drives, or any means necessary to allow full recovery from incidents.[8]

>Table of Contents | >About the Checklist | >Team Worksheet | >About the Practice Worksheets | >Practice Worksheets

Recommended Practice

1.2 An electric generator and sufficient fuel are available to support the EHR during an extended power outage.[9]

Checklist

Implementation Status

Off

Rationale for Practice or Risk Assessment

Most healthcare organizations must be able to continue running their health IT infrastructure and preserve data and communication capabilities in cases of sustained power outages.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

Clinicians, support staff, and/or clinical administration

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- Organizations evaluate the consequences to patient safety and to business operations due to loss of power that shuts down the EHR, and implement concrete plans to keep the EHR running to the extent needed to avoid unacceptable consequences.
- In the event of a power failure, there is an uninterruptible power supply (UPS), either batteries or a "flywheel," capable of providing instantaneous power to maintain the EHR for at least 10 minutes.
- The UPS is tested regularly (optimally on at least a monthly basis).
- The on-site, backup electrical generator is able to maintain EHR functions critical to the organization's operation (e.g., results review, order entry, clinical documentation).[10]
- The organization maintains 2 days of fuel for the generator on-site.
- The generator is tested regularly (optimally at least on a monthly basis).
- The UPS and the generator are kept in secure locations that are not likely to flood.

Recommended Practice

1.3 Paper forms are available to replace key EHR functions during downtimes.[11]
Checklist

Implementation Status

Off

Rationale for Practice or Risk Assessment

Clinical and administrative operations need to continue in the event of a downtime.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

Clinicians, support staff, and/or clinical administration

Examples of Potentially Useful Practices/Scenarios

- The organization maintains enough paper forms to care for patients on an in-patient unit for at least 8 hours. Paper forms could include those required to enter orders and document the administration of medications, labs, and radiology on each unit.[12]
- There is a process in place to ensure that the information recorded on paper during the downtime gets entered and reconciled into the EHR following its reactivation (e.g., entering information as coded data, scanning of paper documents).[12]

Recommended Practice

1.4 Patient data and software application configurations critical to the organization's operations are backed up.[13]

Checklist

Implementation Status

Off

Rationale for Practice or Risk Assessment

Backup of mission-critical patient data and EHR system configuration allows system restoration to a "pre-failure" state with minimal data loss. In the event of failure, you are able to rely upon reliable back-up data.

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

- The organization has a daily, off-site, complete, encrypted backup of patient data.[14]
- The off-site backup is tested regularly (i.e., complete restore) (optimally on at least a monthly basis).[15]
- The content required to configure the system is backed up on a regular basis (optimally on a monthly basis and before every system upgrade).
- The organization maintains multiple backups, created at different times.
- Backup media are physically secured.
- Backup media are rendered unreadable (i.e., use software to scramble media contents or physically destroy/shred media) before disposal.
- The organization has a "read-only" backup EHR system that is updated frequently (optimally at least hourly).
- The read-only EHR system is tested regularly (optimally at least weekly).
- Users can print from the read-only EHR system.
- If there is a "unit-level" read-only backup EHR system, it is connected to a local UPS or "red plug" (i.e., an outlet connected to the organization's backup electrical generator).

Recommended Practice

Implementation Status

1.5 Policies and procedures are in place to ensure accurate patient identification when preparing for, during, and after downtimes.
Checklist

Off

Rationale for Practice or Risk Assessment

Without policies, procedures, and processes in place to manage patient identification during downtimes, mismatches and lost records could compromise patient confidentiality, data integrity, and patient safety.

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

Examples of Potentially Useful Practices/Scenarios

- The read-only EHR system should have user-specific passwords (i.e., should not employ a shared password for all users).
- There is a mechanism in place to register new patients during downtime, including assignment of unique temporary patient record numbers along with a process for reconciling these new patient IDs once the EHR comes back online.
- Ensure that paper documents created during downtime are protected using standard HIPAA safeguards and policies.

>Table of Contents | >About the Checklist | >Team Worksheet | >About the Practice Worksheets | >Practice Worksheets

Recommended Practice

2.1 Staff are trained and tested on downtime and recovery procedures.[16]
Checklist

Implementation Status

Off

Rationale for Practice or Risk Assessment

In organizations that have not had a significant downtime in more than a year, there is an increased risk of having employees who do not know how to function in a paper environment.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

Clinicians, support staff, and/or clinical administration

Examples of Potentially Useful Practices/Scenarios

- Organizations establish and follow training requirements so that each employee knows what to do to keep the organization operating safely during EHR downtimes.[17]
- Clinicians are trained in use of the paper-based ordering and charting tools.
- The organization conducts unannounced EHR "downtime drills" at least once a year.[18]
- Clinicians have been trained on how and when to activate and use the "read-only" backup EHR system.[19]

>Table of Contents | >About the Checklist | >Team Worksheet | >About the Practice Worksheets | >Practice Worksheets

Recommended Practice

2.2 A communication strategy that does not rely on the computing infrastructure exists for downtime and recovery periods.
Checklist

Implementation Status

Off

Rationale for Practice or Risk Assessment

The organization needs to be prepared to communicate with key personnel without use of the computer.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

Clinicians, support staff, and/or clinical administration

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- The organization has methods other than electronic (i.e., not email, Twitter, voice-over-IP) to notify key organizational administrators and clinicians about times when the EHR is down (either planned or unplanned).[18, 20]
- The organization has a mechanism in place to activate the read-only backup EHR system and notify clinicians how to access it.
- The organization has a mechanism in place to notify clinicians when the EHR is back on-line (either planned or unplanned).

>Table of Contents | >About the Checklist | >Team Worksheet | >About the Practice Worksheets | >Practice Worksheets

Recommended Practice

2.3 Written policies and procedures on EHR downtimes and recovery processes ensure continuity of operations with regard to safe patient care and critical business operations.[21]

Checklist

Implementation Status

Off

Rationale for Practice or Risk Assessment

Policies and procedures on EHR downtime and recovery keep everyone "on the same page" so they are able to care for patients and maintain critical business operations during inevitable downtimes, whether planned or unplanned.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

Clinicians, support staff, and/or clinical administration

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- The organization has a written EHR downtime and recovery policy that describes key elements such as when a downtime should be called; how often further communication will be delivered; who will be in charge during the downtime (both on the clinical and technical side); how everyone will be notified; and how information collected during the downtime is entered into the EHR.[22]
- The EHR downtime policy is reviewed at least every 2 years.[23]
- The EHR downtime policy describes when the warm-site backup process should be activated (ideally, before the system has been down for 2 hours).
- A paper copy of the current EHR downtime and recovery policy is available on clinical units.
- A paper copy of the current EHR downtime and recovery policy is stored in a safe, off-site location.

Recommended Practice

2.4 The user interface of the locally maintained backup, read-only EHR system is clearly differentiated from the live/production EHR system.

Checklist

Implementation Status

Off

Rationale for Practice or Risk Assessment

When the usual system is unavailable, a read-only copy can enable access to patient records, though it can't support adding or editing patient data. If it looks the same to users it could easily result in attempts to enter data that will not be recorded.

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

Examples of Potentially Useful Practices/Scenarios

- Access to the "read-only" backup EHR is disabled (e.g., icons on the computer screens are "greyed out" or not available) during periods of normal EHR operations.
- The user interface of the read-only backup EHR system is visibly different than the fully operational system (e.g., there is a different background color for screens, a watermark across screens, data entry fields are greyed out).
- Clinicians are trained on appropriate use of the read-only backup EHR.

> Table of Contents | > About the Checklist | > Team Worksheet | > About the Practice Worksheets | > Practice Worksheets

Recommended Practice

2.5 Users are trained on ransomware prevention strategies including how to identify malicious emails.
Checklist

Implementation Status

Off

Rationale for Practice or Risk Assessment

Malicious email attachments are often the first point of entry for ransomware attacks.

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

Examples of Potentially Useful Practices/Scenarios

- The organization trains users to identify spam, phishing, and spear-phishing messages, and users avoid clicking on potentially weaponized attachments (such as *.exe, *.zip, *.rar, *.7z, *.js, *.wsf, *.docm, *.xlsm, *.pptm, *.rtf, *.msi, *.bat, *.com, *.cmd, *.hta, *.scr, *.pif, *.reg, *.vbs, *.cpl, *.jar files). Safe file attachment formats include (*.jpg, *.png, *.pdf, *.docx, *.xlsx, and *.pptx).[24]
- Training should reinforce that legitimate organizational mail messages (e.g., your employer's IT department, your bank, your credit card company, companies you work with) should always meet the following requirements: 1) never ask you to download and run file attachments; 2) never ask for you to enter account or password information; 3) always have a telephone number someone can call (i.e., out-of-band check); 4) always be associated with an email address and name that people can check in their local directory; and 5) contain website links that display the complete internet address (URL) to build trust.
- The organization restricts users' ability to install and run software applications using the principle of "Least Privilege," or minimizes users' access to only those systems and services required by their job.
- The organization considers disabling the USB ports on the organization's computers.[25]
- The organization conducts simulated phishing attacks (i.e., sends fraudulent (but safe) email messages or websites that appear to be from legitimate sources) to raise user's awareness of the problem.

>Table of Contents | >About the Checklist | >Team Worksheet | >About the Practice Worksheets | >Practice Worksheets

Recommended Practice

3.1 There is a comprehensive testing and monitoring strategy in place to prevent and manage EHR downtime events.
Checklist

Implementation Status

Off

Rationale for Practice or Risk Assessment

Comprehensive testing and monitoring strategies can prevent and minimize the impact of technology failures.

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

- The organization regularly monitors and reports on system downtime events.[26]
- The organization regularly monitors and reports on system response time (optimally under 2 seconds) for important clinical tasks (e.g., results review, order entry, patient look-up).[27]
- The organization has a written policy describing the different hardware, software, process, and people-related testing procedures.
- The organization maintains a log of all testing activities.
- Unplanned downtimes and the effectiveness of follow-up to prevent them from recurring are monitored by the top leadership.

> Table of Contents | > About the Checklist | > Team Worksheet | > About the Practice Worksheets | > Practice Worksheets

Recommended Practice

3.2 Functional system downtimes (i.e., unacceptably slow response time) are identified and addressed proactively.
Checklist

Implementation Status

Off

Rationale for Practice or Risk Assessment

Slow computer response times significantly impede user efficiency and can result in “type ahead” errors in which the computer saves commands (e.g., repeated enter key presses) and enters them (unbeknownst to the user) in the default data entry field once the form loads, resulting in unexpected behavior.

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

Examples of Potentially Useful Practices/Scenarios

- Create strategies to calculate system response times. One such strategy is to create an application to submit a simple medication order for a “test patient” every day of the year at midnight and run a simple automated query to request this order’s details be displayed on a workstation in a clinical setting every minute for the next 24 hours (i.e., 1440 times). Mean system response time is the time from order being requested until the time the details are available. Functional system downtime can be defined by any hourly mean response time greater than 5 seconds or 3 standard deviations above the mean.[27]
- The organization creates easy mechanisms for users to report slow system response time to the IT Helpdesk.

Recommended Practice

3.3 Review unexpected extended system downtimes greater than 24 hours using root-cause analysis or similar approaches.[28]

Checklist

Implementation Status

Off

Rationale for Practice or Risk Assessment

Experiences with an unexpected downtime over 24 hours are likely to provide learning opportunities for future management and prevention of similar events.

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

Examples of Potentially Useful Practices/Scenarios

- The organization convenes a multi-disciplinary group of clinicians and IT professionals to review the event and its management, identify potential root causes, and discuss future prevention or mitigating procedures.
- The organization considers consulting with additional experts in IT system reliability to review and report on recommendations for improvements in key system components, configurations, and policies and procedures.

References

1. Kilbridge, P. (2003). Computer crash-lessons from a system failure. New England Journal of Medicine, 348(10), 881-882.

2. Hanuscak, T. L., Szeinbach, S. L., Seoane-Vazquez, E., Reichert, B. J., & McCluskey, C. F. (2009). Evaluation of causes and frequency of medication errors during information technology downtime. American Journal of Health-System Pharmacy, 66(12).

3. McBiles, M., & Chacko, A. K. (2000). Coping with PACS downtime in digital radiology. Journal of Digital Imaging, 13(3), 136-142.

4. Sittig, D. F., & Singh, H. (2012). Electronic health records and national patient-safety goals. New England Journal of Medicine, 367(19), 1854-1860.

5. Lee, O. F., & Guster, D. (2012). Virtualized disaster recovery model for large scale hospital and healthcare systems. Advancing Technologies and Intelligence in Healthcare and Clinical Environments Breakthroughs, 307.

6. Sittig, D. F., & Singh, H. (2011). Defining health information technology-related errors: New developments since To Err Is Human. Archives of Internal Medicine, 171(14), 1281-1284.

7. Dooling, J. A. (2013). Meaningful Use and Disaster Infrastructure Q&A: HIM Professionals Share Lessons Learned. Journal of AHIMA, 84(10), 64-65.

8. Schweitzer, E. J. (2012). Reconciliation of the cloud computing model with US federal electronic health record regulations. Journal of the American Medical Informatics Association, 19(2), 161-165.

9. Jacques, C. C., Boston, M., & Mitrani-Reiser, J. (2014). Quantifying the performance of healthcare facilities in disasters: a multi-hazard approach. Tenth U.S. National Conference on Earthquake Engineering Frontiers of Earthquake Engineering July 21-25, 2014; Anchorage, Alaska.

10. Hiller, M., Bone, E. A., & Timmins, M. L. (2015). Healthcare system resiliency: The case for taking disaster plans further-Part 2. Journal of Business Continuity & Emergency Planning, 8(4), 356-375.

11. Lei, J., Guan, P., Gao, K., Lu, X., Chen, Y., Li, Y., ... & Zheng, K. (2014). Characteristics of health IT outage and suggested risk management strategies: An analysis of historical incident reports in China. International Journal of Medical Informatics, 83(2), 122-130.

12. McKinney, M. (2007). Technology. What happens when the IT system goes down? Hospitals & Health Networks/AHA, 81(12), 14.

13. Sittig, D. F., Gonzalez, D., & Singh, H. (2014). Contingency planning for electronic health record-based care continuity: a survey of recommended practices. International Journal of Medical Informatics, 83(11), 797-804.

14. Piliouras, T. C., Suss, R. J., & Yu, P. L. (2015, May). Digital imaging & electronic health record systems: Implementation and regulatory challenges faced by healthcare providers. In Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island (pp. 1-6). IEEE.

15. Schackow, T. E., Palmer, T., & Epperly, T. (2008). EHR meltdown: how to protect your patient data. Family Practice Management, 15(6), A3.

16. Brazelton, N. C., & Lyons, A. (2014). Health Information Systems: Downtime and Disaster Recovery. PROP-Healthcare Information Systems Custom, 256.

17. Oral, B., Cullen, R. M., Diaz, D. L., Hod, E. A., & Kratz, A. (2015). Downtime Procedures for the 21st Century. American Journal of Clinical Pathology,143(1), 100-104.

18. Genes, N., Chary, M., & Chason, K. W. (2013). An academic medical center's response to widespread computer failure. American Journal of Disaster Medicine, 8(1), 2.

19. Poterack, K. A., & Gottlieb, O. (2016). Are you ready for EHR downtime? Questions to ask. ASA Newsletter, 80(2), 30-31.

References

20. Nelson, N. C. (2007). Downtime procedures for a clinical information system: a critical issue. Journal of Critical Care, 22(1), 45-50.

21. Menon, S., Singh, H., Meyer, A. N., Belmont, E., & Sittig, D. F. (2014). Electronic health record-related safety concerns: A cross-sectional survey. Journal of Healthcare Risk Management, 34(1), 14-26.

22. Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smith, C., & Steinberg, D. (2008). An introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. NIST Special Publications 800-66 Revision 1; October 2008.

23. Fernández, M. T., Gómez, A. R., Santojanni, A. M., Cancio, A. H., Luna, D. R., & Benítez, S. E. (2014). Electronic Health Record System Contingency Plan Coordination: A Strategy for Continuity of Care Considering Users' Needs. Studies in Health Technology and Informatics, 216, 472-476.

24. Hoffman, C. (2014). How To Spot A Dangerous Email Attachment. Make Use Of (a website).

25. Wright, A., & Sittig, D. F. (2007). Security threat posed by USB-based personal health records. Annals of Internal Medicine, 146(4), 314-315.

26. Blecker, S., Austrian, J. S., Shine, D., Braithwaite, R. S., Radford, M. J., & Gourevitch, M. N. (2013). Monitoring the pulse of hospital activity: electronic health record utilization as a measure of care intensity. Journal of Hospital Medicine, 8(9), 513-518.

27. Sittig, D. F., Campbell, E. M., Guappone, K. P., Dykstra, R. H., & Ash, J. S. (2007, October). Recommendations for Monitoring and Evaluation of In-Patient Computer-based Provider Order Entry Systems: Results of a Delphi Survey. In AMIA.

28. Sittig DF, Singh H. (2010, May). (author reply) Monitoring and evaluating the use of electronic health records. JAMA. 303(19): 1918-9.