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 (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

# 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,[2] represents a significant potential patient safety hazard that directly affects patient care. Documented potential hazards include an increased risk of medication errors,[3] unavailability of images,[4] and canceled procedures. The potential impact of EHR unavailability increases as such systems are deployed across multiple, geographically dispersed facilities within a healthcare system.[1] 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 *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 | 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 downtimes 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 downtime events. | *Worksheet 10* | ○ | ○ | ○ | 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

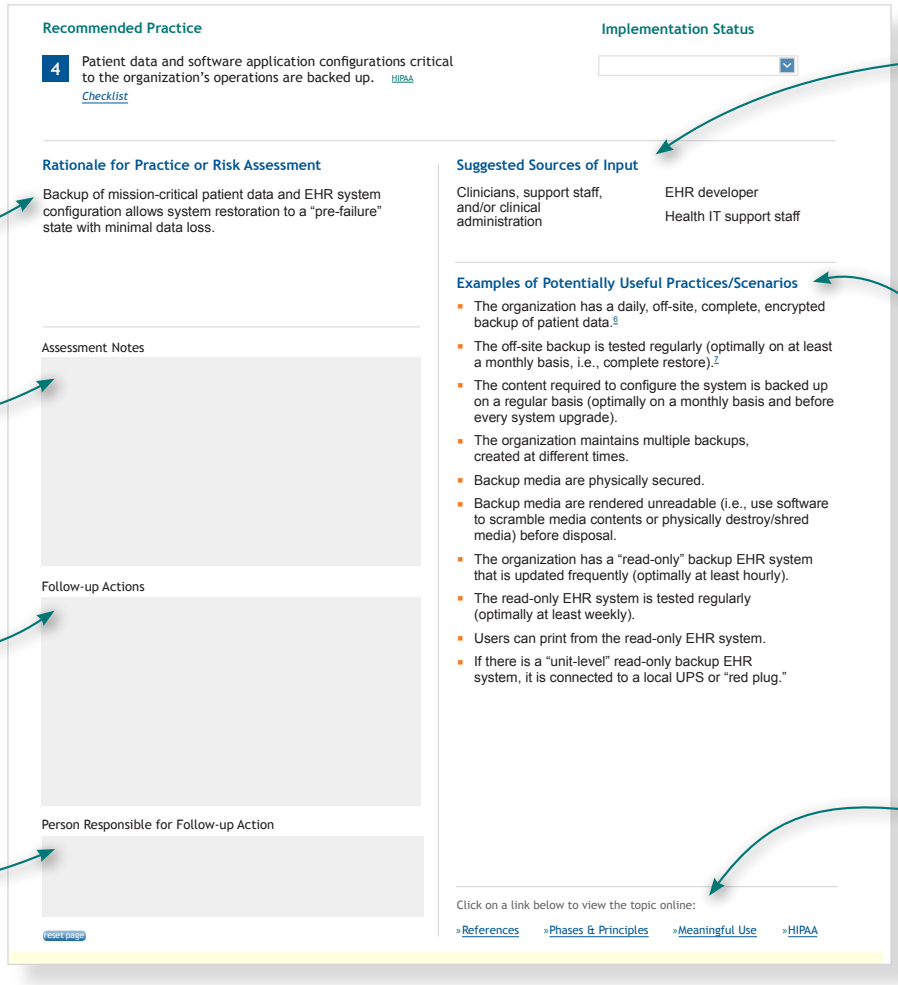
Each *Worksheet* provides guidance on implementing a specific *Recommended Practice*, and allows you to enter and print information about your self-assessment.

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

*Checklist*

## Implementation Status

## 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

- The organization 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.[12]

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

## Recommended Practice

**2** An electric generator and sufficient fuel are available to support the EHR during an extended power outage. HIPAA

*Checklist*

## Implementation Status

## 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.

## 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).
- 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.

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** Paper forms are available to replace key EHR functions during downtimes. HIPAA

*Checklist*

## Implementation Status

## Rationale for Practice or Risk Assessment

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

## 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 the 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.[8]
- 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., this could be entering information as coded data or scanning of paper documents).[8]

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

**4** Patient data and software application configurations critical to the organization's operations are backed up. HIPAA

*Checklist*

## Implementation Status

## 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.[6]
- The off-site backup is tested regularly (optimally on at least a monthly basis, i.e., complete restore).[7]
- 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."

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

## Recommended Practice

**5** Policies and procedures are in place to ensure accurate patient identification when preparing for, during, and after downtimes. HIPAA

*Checklist*

## Implementation Status

## 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.

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

## Recommended Practice

**6** Staff are trained and tested on downtime and recovery procedures. HIPAA

*Checklist*

## Implementation Status

## 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.

## 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.
- 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.[8]
- Clinicians have been trained on how and when to activate and use the "read-only" backup EHR 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

**7** A communication strategy that does not rely on the computing infrastructure exists for downtime and recovery periods. HIPAA

*Checklist*

## Implementation Status

## Rationale for Practice or Risk Assessment

Institutions need 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, etc.) to notify key organizational administrators and clinicians about times when the EHR is down (either planned or unplanned).[9]
- 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).

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

## Recommended Practice

**8** Written policies and procedures on EHR downtimes and recovery processes ensure continuity of operations with regard to safe patient care and critical business operations. HIPAA

*Checklist*

## Implementation Status

## 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.

## 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.[10]
- The EHR downtime policy is reviewed at least every 2 years.
- 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.

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

*Checklist*

## Implementation Status

## 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, or data entry fields are greyed out).
- Clinicians are trained on appropriate use of the read-only backup EHR.

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

## Recommended Practice

**10** There is a comprehensive testing and monitoring strategy in place to prevent and manage EHR downtime events. HIPAA

*Checklist*

## Implementation Status

## Rationale for Practice or Risk Assessment

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

## 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.
- The organization regularly monitors and reports on system response time (optimally under 2 seconds).[11]
- 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.

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