Self Assessment

# System Configuration

## 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 Configuration

## Introduction

The *System Configuration SAFER Guide* identifies recommended safety practices associated with the way EHR hardware and software are set up ("configured"). EHR configuration includes the creation and maintenance of the physical environment in which the system will operate, as well as the implementation of the required hardware and software infrastructure. Working through this guide with a multi-disciplinary team will focus the team's attention on configuration-related recommended practices to optimize the safety and safe use of the EHR.

Configuration of an EHR's hardware and software components within a particular environment is complex and vulnerable to errors. EHRs are profoundly influenced by their configuration, and numerous decisions must be made with the configuration team. Generally, the team should include practicing clinicians to ensure that technical components align with and support the clinical processes and workflows impacted by their decisions. In addition to the substantial initial configuration effort, a continuous, reliable configuration review and maintenance process must be developed and followed. EHR safety and effectiveness can be improved by establishing proper configuration procedures, policies, and practices.

Completing the self-assessment in the *System Configuration 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 EHR-related safety concerns, clinician leadership in the organization should be engaged to assess 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 EHR configuration 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 mitigate the highest priority configuration-related safety risks introduced by the EHR.

Self Assessment

# System Configuration

## 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.

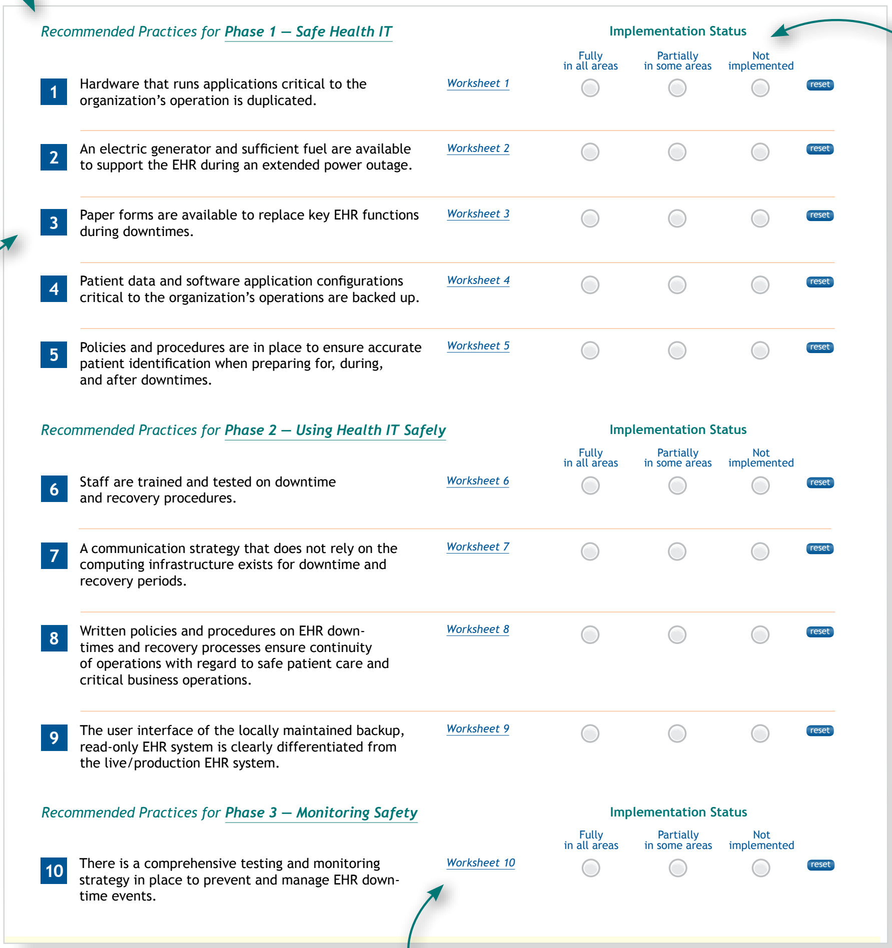
The ONC composite mark is a mark of the U.S. Department of Health and Human Services. The contents of the publication or project are solely the responsibility of the authors and do not necessarily represent the official views of the U.S. Department of Health and Human Services, Office of the National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

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

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 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 |

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<br>in all areas | Partially<br>in some areas | Not<br>implemented | |
| 1 | There are an adequate number of EHR access points in all clinical areas. | *Worksheet 1* | ○ | ○ | ○ | reset |
| 2 | The EHR is hosted safely in a physically and electronically secure manner. | *Worksheet 2* | ○ | ○ | ○ | reset |
| 3 | The organization's information assets are protected using strong person authentication mechanisms. | *Worksheet 3* | ○ | ○ | ○ | reset |
| 4 | System hardware and software required to run the EHR (e.g., operating system) and their modifications are tested individually and as-installed before go-live and are closely monitored after go-live. | *Worksheet 4* | ○ | ○ | ○ | reset |
| 5 | Clinical applications and system interfaces are tested individually and as-installed before go-live and are closely monitored after go-live. | *Worksheet 5* | ○ | ○ | ○ | reset |
| 6 | Computers and displays in publicly accessible areas are configured to ensure that patient identifiable data are physically and electronically protected. | *Worksheet 6* | ○ | ○ | ○ | reset |
| 7 | There are processes in place to ensure data integrity during and after major system changes, such as upgrades to hardware, operating systems, or browsers. | *Worksheet 7* | ○ | ○ | ○ | reset |

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

| | | | Implementation Status | | | |
|---|---|---|---|---|---|---|
| | | | Fully<br>in all areas | Partially<br>in some areas | Not<br>implemented | |
| 8 | Clinical content used, for example, to create order sets and clinical charting templates and to generate reminders within the EHR, is up-to-date, complete, available, and tested. | *Worksheet 8* | ○ | ○ | ○ | reset |
| 9 | There is a role-based access system in place to ensure that all applications, features, functions, and patient data are accessible only to users with the appropriate level of authorization. | *Worksheet 9* | ○ | ○ | ○ | reset |

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

| | | | Implementation Status | | | |
|---|---|---|---|---|---|---|
| | | | Fully in all areas | Partially in some areas | Not implemented | |
| 10 | The EHR is configured to ensure EHR users work in the "live" production version, and do not confuse it with training, test, and read-only backup versions. | *Worksheet10* | ○ | ○ | ○ | reset |
| 11 | System configuration settings that limit clinical practice are minimized, carefully implemented following clinician acceptance, and closely monitored. | *Worksheet 11* | ○ | ○ | ○ | reset |
| 12 | The human-computer interface is configured for optimal usability for different users and clinical contexts. | *Worksheet 12* | ○ | ○ | ○ | reset |

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

| | | | Implementation Status | | | |
|---|---|---|---|---|---|---|
| | | | Fully in all areas | Partially in some areas | Not implemented | |
| 13 | The organization has processes and methods in place to monitor the effects of key configuration settings to ensure they are working as intended. | *Worksheet 13* | ○ | ○ | ○ | 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

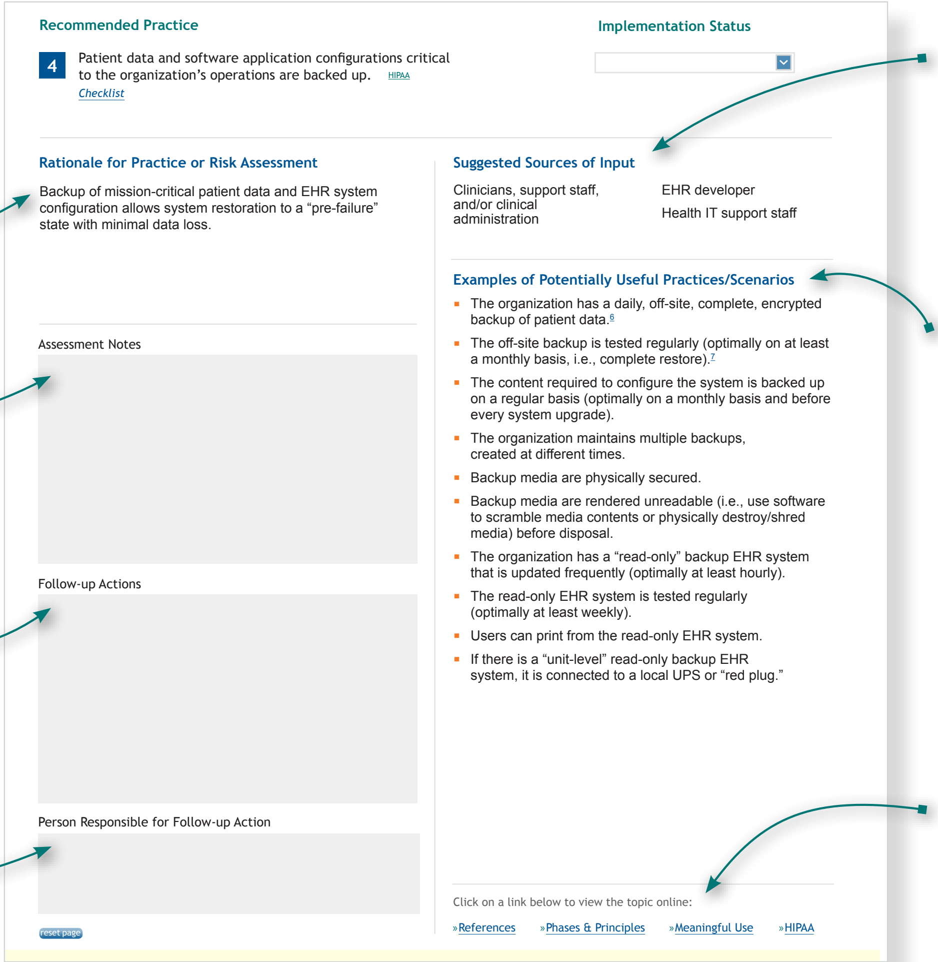
Each *Worksheet* provides guidance on implementing a specific *Recommended Practice*, and allows you to enter and print information about your self-assessment.

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.



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.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

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 »Meaningful Use »HIPAA

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.

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

## Recommended Practice

**1** There are an adequate number of EHR access points in all clinical areas. HIPAA

*Checklist*

## Implementation Status

## Rationale for Practice or Risk Assessment

Rapid, reliable access to the patient's computer-based record is essential for safe and effective care. Such access depends critically on configuring the EHR in clinical care areas such that a computer is always conveniently available.

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

- Organizational policy sets minimum standards for EHR access by clinicians (e.g., clinicians walk no more than 50 feet to access an EHR and, if there are wait times, they are minimal and ensure that urgent clinical needs can be addressed).
- Resources are dedicated to acquiring sufficient computer hardware to ensure appropriate access, in accordance with policy.
- Workflows have been mapped to ensure ready and timely access to all needed EHR functionality in clinical areas.
- There is at least one EHR access point for every clinician and administrative staff member in an outpatient clinic.[5]
- Computer terminals used to access the EHR are mapped to the appropriate (e.g., a nearby) printer.
- There is at least one printer available for use on all acute care nursing units or within easy reach of each outpatient exam room (e.g., less than 25 feet).
- There is a mapping table that shows the physical location of all hard-wired, network-attached devices (end-user workstations and printers).
- Critical hardware is connected to a regularly tested uninterruptible power supply (UPS).[1]
- Clinicians should not have to wait for or walk more than 50 feet on a clinical unit to find an available EHR access point.

Click on a link below to view the topic online:

»References »Phases & Principles »Meaningful Use »HIPAA

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

## Recommended Practice

**2** The EHR is hosted safely in a physically and electronically secure manner.

Meaningful Use HIPAA

*Checklist*

## Implementation Status

## Rationale for Practice or Risk Assessment

Whether the EHR is hosted locally or remotely, it can only provide reliable support for safe, effective care if it is available and secure.

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

- Key data required to take care of patients and run the organization are available 24 hours/7 days per week, are not altered inadvertently or maliciously, and are kept confidential.
- All data and operational systems are maintained on at least two geographically distinct hosting sites that are mirrored in real-time (“hot” or “warm” sites). This redundancy reduces the risk of a single natural or man-made disaster to disable operating capacity.
- There are at least two physically distinct network connections between the hosting sites.
- Within a data center (i.e., hosting center), all servers are mirrored on physically separate servers.
- The healthcare organization has a contract in place that describes in detail how they will get functional access to their data in the event that either the EHR system developer or the remote hosting site goes out of business (e.g., EHR and database management software has been placed in escrow, and current data backups are independently accessible).[2]
- In an EHR’s shared, remote hosting facility the data from different healthcare organizations are maintained within separate virtual machine (VM) environments or on separate physical servers.

Click on a link below to view the topic online:

»References »Phases & Principles »Meaningful Use »HIPAA

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

## Recommended Practice

**3** The organization’s information assets are protected using strong person authentication mechanisms. Meaningful Use HIPAA

*Checklist*

## Implementation Status

## Rationale for Practice or Risk Assessment

Failure to implement and manage secure processes to authenticate access to any system or data (e.g., strong passwords, fingerprints, and role-based access) is an avoidable source of erroneous data that can lead to patient harm.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

## Suggested Sources of Input

Health IT support staff

## Examples of Potentially Useful Practices/Scenarios

- Organizations have policies and procedures and conduct regular risk assessments to define, implement, and monitor person authentication.
- Access to the organization’s “backbone network” via wireless devices is password protected.
- Two-factor authentication is required for remote access to the servers’ “administrative” accounts (e.g., root privileges on Unix) and clinicians’ remote access to patient data. There are three types of authentication, often described as something you know, have, or are. Two-factor authentication involves using at least two means of identification, information one knows (i.e., password), information one has (i.e., electronic ID card or random number token), or information unique to a person (e.g., biometric such as iris or fingerprint scan).
- All users have a unique username and “strong” password (e.g., contains letters, numbers, and special characters). Periodic changes to passwords are required.[3]
- Employee login credentials are revoked as soon as their employment ends.
- The organization has implemented a “single sign-on” solution that allows authorized clinicians to rapidly move between disparate clinical applications without requiring additional login information.[4]

Click on a link below to view the topic online:

»References »Phases & Principles »Meaningful Use »HIPAA

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

## Recommended Practice

**4** System hardware and software required to run the EHR (e.g., operating system) and their modifications are tested individually and as-installed before go-live and are closely monitored after go-live. HIPAA

*Checklist*

## Implementation Status

## Rationale for Practice or Risk Assessment

Failure to adequately test system hardware and software can lead to suboptimal performance as measured by response time, reliability, and error-free operation.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

## Suggested Sources of Input

Health IT support staff

## Examples of Potentially Useful Practices/Scenarios

- Critical system infrastructure components, such as database servers, network routers, and end-user terminals are regularly load tested.
- All system software updates are installed and tested in the "test" environment before they are moved into the production or "live" environment and re-tested.
- The organization monitors system downtime and response time.[5]
- Organizational policies and procedures address post-installation issues (e.g., 24x7 support, help desk availability, and leadership walk-arounds).[10]
- Organizational policies define criteria for testing (e.g., testing in a simulated environment, day of week testing, minimum # of test cases, types of user roles associated with test cases, facility defined vs. developer defined test cases).

Click on a link below to view the topic online:

» References » Phases & Principles » Meaningful Use » HIPAA

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

## Recommended Practice

## Implementation Status

**5** Clinical applications and system interfaces are tested individually and as-installed before go-live and are closely monitored after go-live. HIPAA

*Checklist*

## Rationale for Practice or Risk Assessment

One of the most common sources of adverse events is poor configuration between critical applications, such as between CPOE and pharmacy. Failure to adequately test applications and their interfaces can lead to data integrity issues as well as impede response time, availability, and error-free operation.

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

- New application software and updates (both major upgrades and small “patches”) are installed and tested in the “test” environment before they are moved into the production or “live” environment, then re-tested and closely monitored in the “live” environment for several days.
- System-system interfaces between key clinical applications (e.g., CPOE and pharmacy, or laboratory and EHR) are tested and continuously monitored to detect new errors.
- Simulations are conducted for clinical processes such as order entry, pharmacy review, nurse notification, medication fill, medication administration, and nursing documentation to ensure that the application addresses the organization’s needs.

Click on a link below to view the topic online:

» References » Phases & Principles » Meaningful Use » HIPAA

## Recommended Practice

6 Computers and displays in publicly accessible areas are configured to ensure that patient identifiable data are physically and electronically protected. HIPAA

Checklist

## Implementation Status

## Rationale for Practice or Risk Assessment

Failure to physically protect patient identifiable data to ensure that it is not inadvertently or maliciously viewed, changed, or deleted is vital to ensuring safe and effective use of clinical applications.

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

- Terminals used to access patient data in publicly accessible locations have an automatic screen locking feature set, appropriate to the clinical setting (e.g., lock after idle for three minutes).
- Devices used to access patient data have their screens facing away from publicly accessible locations and/or have “privacy filters” (i.e., filters that restrict screen viewing angles).
- Public displays of patient names on EHRs are masked (i.e., only a portion of the patient’s name is visible in public areas, e.g., ED and waiting rooms).
- The server room has physical security controls in place (e.g., room is locked, there is non-water-based fire suppression, room is above ground to prevent flooding, and backups are kept in a different location).
- All portable computing devices used to access EHR data have encrypted hard drives.
- Backups containing patient-identifiable data are encrypted.

Click on a link below to view the topic online:

»References »Phases & Principles »Meaningful Use »HIPAA

## Recommended Practice

## Implementation Status

7 There are processes in place to ensure data integrity during and after major system changes, such as upgrades to hardware, operating systems, or browsers. HIPAA

Checklist

## Rationale for Practice or Risk Assessment

Major system changes create the risk of loss or corruption of patient data. Data persistence must be ensured independent of hardware and software changes to maintain continuity of care. Losing data due to "improvements" in the underlying systems is unacceptable.

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 have change management and internal control policies and procedures in place, designed to ensure data integrity, which apply to all major system changes. Major system changes include, at a minimum, operating system or browser version upgrades, or adding new system software (e.g., virus protection upgrades).
- There are processes in place to migrate existing data to the new system while ensuring it remains accurate, valid, and accessible after changes to the:
  - application (e.g., from one EHR system to another),
  - format (e.g., from free text to structured data),
  - coding system (e.g., from ICD-9 to ICD-10),
  - storage mechanism (e.g., from magnetic tapes to solid state hard drives), etc.
- Standard clinical and administrative reports are generated and reviewed regularly to ensure that the data on which they are based has not changed in a way that renders the report meaningless.
- If data becomes corrupted, the facility has policies and processes for reverting to a backup version of the data that precedes the corruption.

Click on a link below to view the topic online:

» References » Phases & Principles » Meaningful Use » HIPAA

## Recommended Practice

## Implementation Status

**8** Clinical content used, for example, to create order sets and clinical charting templates and to generate reminders within the EHR, is up-to-date, complete, available, and tested.

*Checklist*

### Rationale for Practice or Risk Assessment

Clinical content drives significant parts of the user experience. Failure to update, test, and maintain this content can result in significant degradations in performance.

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

- There are no "broken links" to internet-based clinical information resources.
- The organization has a naming convention and unambiguous synonyms for common orders, results, procedures, order sets, charting templates, and macros (e.g., dot phrases or "canned text").[6]
- Default values are available for common orders (e.g., medication order sentences or routine laboratory draw times).
- Items necessary to provide clinical care are available as orderable items within the CPOE system.
- Clinical content is tested to ensure that items entered in one system are accurately transmitted through the system-to-system interface and received by the remote system unchanged.
- Clinical content is reviewed by the organization at least annually.
- The organization has a clinical informatics committee to review content.

Click on a link below to view the topic online:

»References »Phases & Principles »Meaningful Use »HIPAA

## Recommended Practice

## Implementation Status

9 There is a role-based access system in place to ensure that all applications, features, functions, and patient data are accessible only to users with the appropriate level of authorization. HIPAA

Checklist

## Rationale for Practice or Risk Assessment

Role-based access helps ensure that users can only see, enter, or modify data when necessary to perform their jobs. Organizations are expected to configure and maintain the correct associations between the roles and the functions of the EHR and maintain correct assignments of user roles.

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

- User roles with different data input and review capabilities are defined for both clinical and non-clinical users. Within each of these groups, subcategories of users are defined with very specific capabilities (e.g., only credentialed MDs, DOs, or NPs can order Schedule 2 medications without a co-signature).
- There is a multi-disciplinary committee responsible for creating new roles and determining that the appropriate features and functions are assigned to each role.
- Employees who change jobs are reassigned to the appropriate roles promptly.
- Periodically (e.g., yearly), supervisors are prompted to review and re-authorize or revoke their clinical and administrative staff members' roles and specific authorizations to access various clinical systems and functions.

Click on a link below to view the topic online:

» References » Phases & Principles » Meaningful Use » HIPAA

## Recommended Practice

## Implementation Status

**10** The EHR is configured to ensure EHR users work in the “live” production version, and do not confuse it with training, test, and read-only backup versions. HIPAA

*Checklist*

## Rationale for Practice or Risk Assessment

Failure to clearly differentiate training, testing, and live EHR environments can lead to data review and entry 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

Health IT support staff

## Examples of Potentially Useful Practices/Scenarios

- There is a dedicated “training” environment for the EHR that includes de-identified patient data to allow high-fidelity testing with real-world data.
- Both the training and test environments are as complete as possible (e.g., within the training and test environments users can enter and sign orders that will display for another user, review laboratory data, and see alerts firing appropriately).
- There is a dedicated “test” environment for the EHR that facilitates the configuration and testing of all new software and hardware updates.
- The read-only backup system is password protected and clearly identifiable as read-only.
- The EHR is configured to make it difficult to confuse the live version of the EHR with other versions. For example, the screen background color or the color of the patient headers could be different.
- The organization has a policy and process for creating and naming test patients.  Avoid “cute” names like Dr. Spock, and instead use unmistakable test names like “ZZZ” as a prefix for the name and at least 4 leading zeroes for Medical record number.

Click on a link below to view the topic online:

»References »Phases & Principles »Meaningful Use »HIPAA

## Recommended Practice

**11** System configuration settings that limit clinical practice are minimized, carefully implemented following clinician acceptance, and closely monitored. HIPAA

*Checklist*

## Implementation Status

## Rationale for Practice or Risk Assessment

Configuration decisions that result in mismatches between institutional policies, routine practices, and EHR settings often result in "work-arounds" by clinicians, which increase patient safety risks and lead to suboptimal use of EHRs.

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

- Organizational policies on EHR change/configuration management that address decisions that limit clinical practice, such as mandatory clinical alert settings (e.g., hard stops that cannot be overridden by clinicians or alerts that cannot be turned off by clinicians), are developed with clinicians, and are judiciously implemented and carefully monitored.[7]
- Organizational policy minimizes configurations that limit clinicians' ability to continue practicing (e.g., enter new orders) due to incomplete work (e.g., overdue co-signatures or incomplete discharge summaries).

Click on a link below to view the topic online:

»References »Phases & Principles »Meaningful Use »HIPAA

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

## Recommended Practice

**12** The human-computer interface is configured for optimal usability for different users and clinical contexts. Meaningful Use

*Checklist*

## Implementation Status

## Rationale for Practice or Risk Assessment

Failure to support differences in user interface requirements for different locations, specialties, and users can lead to suboptimal system safety and effectiveness.

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 EHR user interface (those aspects of an EHR that users see and use) is configured (and configurable) to enable users with different capabilities and requirements to use the system safely and effectively (e.g., fonts large enough for all users to see; reduced screen brightness on night shifts; variable color and contrast schemes to accommodate color-blind users).
- The EHR user interface is monitored for safe use (e.g., user-reported usability hazards) and user satisfaction, and is improved over time.
- Default column widths are set wide enough to see key data.
- The EHR user interface is configured to address clinical specialty requirements. Clinical specialties have their “favorites” or 20 most commonly ordered medications, clinical laboratory, and imaging tests available on a single screen.

Click on a link below to view the topic online:

»References »Phases & Principles »Meaningful Use »HIPAA

## Recommended Practice

## Implementation Status

**13** The organization has processes and methods in place to monitor the effects of key configuration settings to ensure they are working as intended. HIPAA *Checklist*

## Rationale for Practice or Risk Assessment

Failure to monitor configuration settings associated with key clinical components (e.g., CPOE interface to pharmacy) and processes (e.g., medication reconciliation) can lead to serious safety events that are otherwise difficult to identify.

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

- Key configuration settings include the number and size of database servers dedicated to the EHR application, password strength, system timeouts, and other similar settings. Organizations have policies and procedures that identify the key configuration settings and the persons responsible for monitoring them.
- The organization has a method of automatically monitoring (e.g., by periodically checking) all internet-based links presented within the EHR.
- System response time is measured and reported regularly.
- The interface error log is regularly reviewed and all errors are identified and fixed promptly.
- The alert override rate is monitored and regularly reviewed. Alerts that are ignored 100 percent of the time (or nearly so) are re-evaluated and fixed or disabled.[8]
- Clinical decision support is monitored using statistical processes (e.g., control charts) to identify malfunctions.[9]

Click on a link below to view the topic online:

»References »Phases & Principles »Meaningful Use »HIPAA