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 (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

# System Configuration

## Introduction

The *System Configuration SAFER Guide* identifies recommended safety practices associated with the way EHR hardware and software are set up (i.e., "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 by the multi-disciplinary configuration team. Generally, this 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. For example, periodic system review and improvements are necessary to maximize the potential benefits of the EHR, and these changes are often less disruptive to business operations and more likely to be successful if implemented through coordinated change management processes. 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 (e.g., EHR technology developers). Because this guide is designed to help organizations prioritize EHR-related safety concerns, clinician leadership in the organization should be engaged 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

General Instructions 1
Introduction 2
About the Checklist 4
Checklist 5
Team Worksheet 7
About the Recommended Practice Worksheets 8
Worksheets 9
References 22

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.*

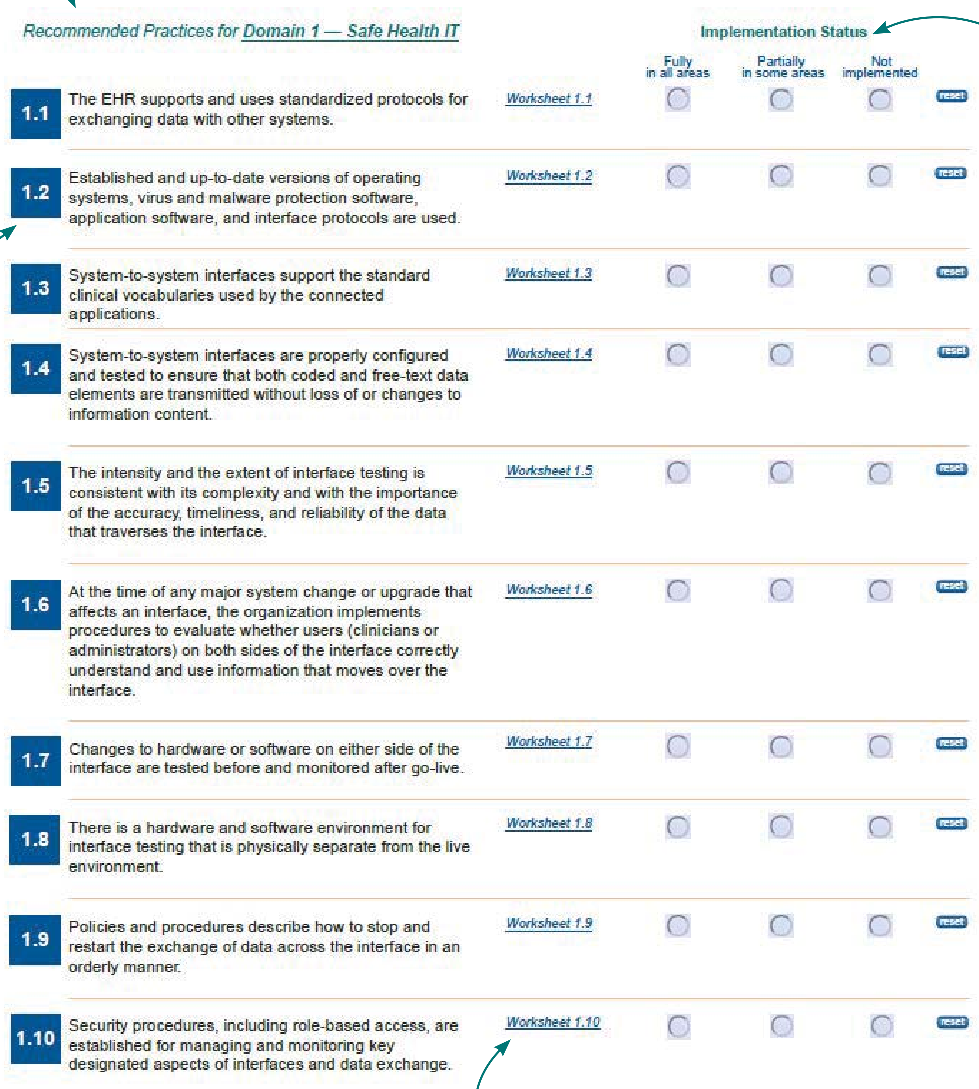
This guide was developed under the contract Unintended Consequences of Health IT and Health Information Exchange, Task Order HHSP23337003T/HHSP23320095655WC.

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.

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 status 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.

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

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

| | | | Implementation Status | | | |
|---|---|---|---|---|---|---|
| | | | Fully in all areas | Partially in some areas | Not implemented | |
| **1.1** | There are an adequate number of EHR access points in all clinical areas. | *Worksheet 1.1* | ○ | ○ | ○ | reset |
| **1.2** | The EHR is hosted safely in a physically and electronically secure manner. | *Worksheet 1.2* | ○ | ○ | ○ | reset |
| **1.3** | The organization's information assets are protected using strong authentication mechanisms. | *Worksheet 1.3* | ○ | ○ | ○ | reset |
| **1.4** | 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 1.4* | ○ | ○ | ○ | reset |
| **1.5** | Clinical applications and system interfaces are tested individually and as-installed before go-live and are closely monitored after go-live. | *Worksheet 1.5* | ○ | ○ | ○ | reset |
| **1.6** | Computers and displays in publicly accessible areas are configured to ensure that patient identifiable data are physically and electronically protected. | *Worksheet 1.6* | ○ | ○ | ○ | reset |
| **1.7** | 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 1.7* | ○ | ○ | ○ | reset |

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

| | | | Implementation Status | | | |
|---|---|---|---|---|---|---|
| | | | Fully in all areas | Partially in some areas | Not implemented | |
| **2.1** | 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 2.1* | ○ | ○ | ○ | reset |
| **2.2** | 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 2.2* | ○ | ○ | ○ | reset |

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

| | | | Implementation Status | | | |
|---|---|---|---|---|---|---|
| | | | Fully<br>in all areas | Partially<br>in some areas | Not<br>implemented | |
| **2.3** | 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. | *Worksheet 2.3* | ○ | ○ | ○ | reset |
| **2.4** | System configuration settings that limit clinicians in their practice are minimized, carefully implemented following clinician acceptance, and closely monitored. | *Worksheet 2.4* | ○ | ○ | ○ | reset |
| **2.5** | The human-computer interface is configured for optimal usability for different users and clinical contexts. | *Worksheet 2.5* | ○ | ○ | ○ | reset |

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

| | | | Implementation Status | | | |
|---|---|---|---|---|---|---|
| | | | Fully<br>in all areas | Partially<br>in some areas | Not<br>implemented | |
| **3.1** | The organization has processes and methods in place to monitor the effects of key configuration settings to ensure they are working as intended. | *Worksheet 3.1* | ○ | ○ | ○ | reset |

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

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

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

Assessment Team Leader

Assessment Completion Date

Assessment Team Members

Assessment Team Notes

reset page

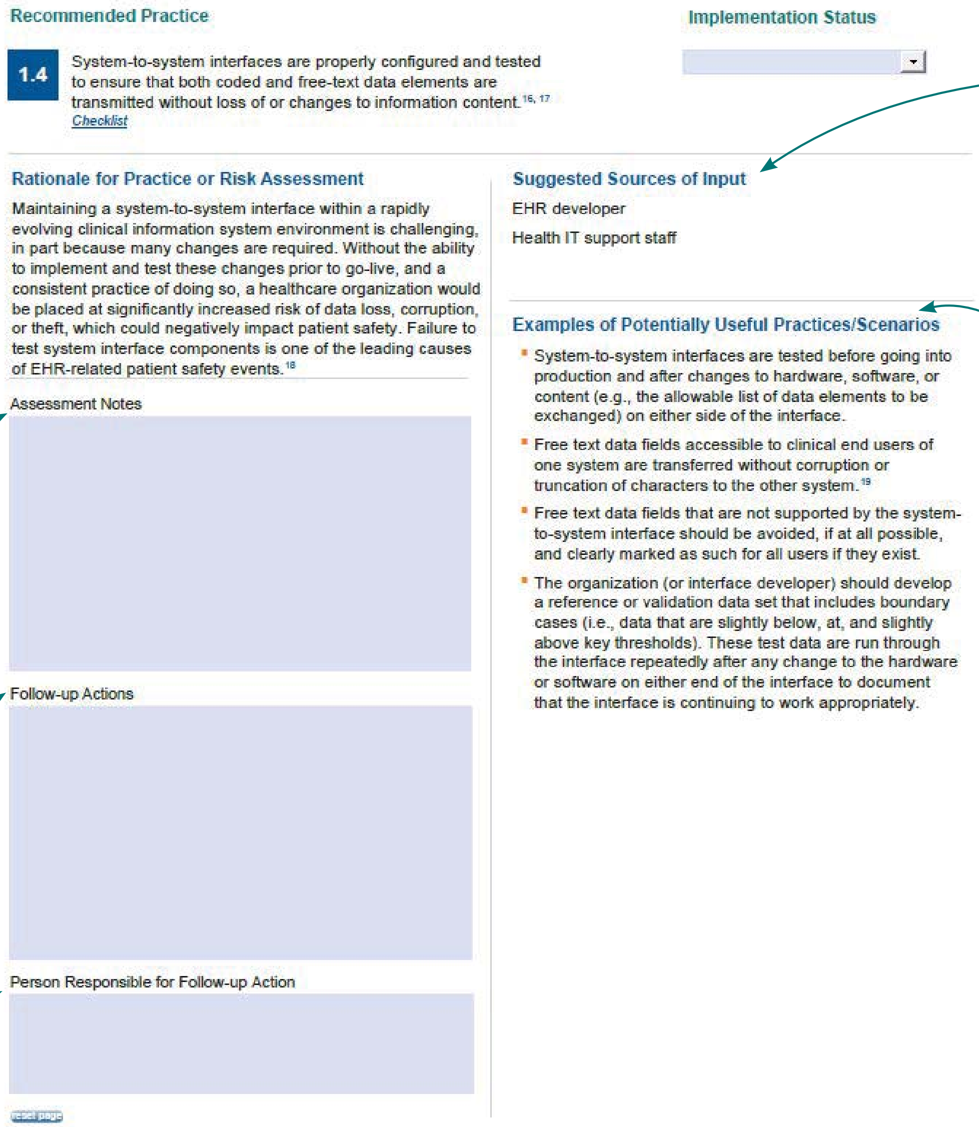
Each *Recommended Practice Worksheet* provides guidance on implementing a specific *Recommended Practice,* and allows you to enter and print information about your self-assessment.

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

Enter any notes about your self-assessment.

Enter any follow-up activities required.

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



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.[15, 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 *Suggested Sources of Input* section indicates categories of personnel who can provide information to help evaluate your status of implementation.

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

## Recommended Practice

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

*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; if there are waiting lines for access, 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 (i.e., both physical and logical) have been mapped to ensure ready and timely access devices and 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.[2]
- 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 (e.g., end-user workstations, printers).
- Critical hardware is connected to a regularly tested uninterruptible power supply (UPS).[3]

## Recommended Practice

## Implementation Status

**1.2** The EHR is hosted safely in a physically and electronically secure manner.[4]
*Checklist*

### 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 per day and 7 days per week, are not altered inadvertently or maliciously, and are kept confidential.
- If the organization requires 24 hour per day, 7 day per week, 365 day per year access to their data, data and operational systems are maintained on at least two geographically distinct hosting sites that are mirrored in real-time (i.e., “hot” or “warm” sites).[5] 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, current data backups are independently accessible).[6]
- When multiple EHRs are being hosted on a remote hosting facility, the data from different healthcare organizations are maintained within separate virtual machine (VM) environments or on separate physical servers.[7]

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

## Recommended Practice

## Implementation Status

**1.3** The organization’s information assets are protected using strong authentication mechanisms.[8]

*Checklist*

## 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, 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

- The organization has policies and procedures and conducts regular risk assessments to define, implement, and monitor 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, something you have, or something you 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).[9]
- All users have a unique username and “strong” password (e.g., contains letters, numbers, special characters). Periodic changes to passwords are required.[10]
- Employee login credentials are revoked as soon as their employment ends.
- To the extent possible, 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.[11, 12]

## Recommended Practice

## Implementation Status

**1.4** 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.[13]
*Checklist*

### 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.[14]
- The organization monitors system downtime and response time.[2]
- Organizational policies and/or procedures address post-installation potential safety hazards (e.g., 24 hour per day and 7 day per week support, help desk availability, leadership walk-arounds).[15]
- Organizational policies and/or procedures define criteria for testing (e.g., testing in a simulated environment, day of week testing, minimum number of test cases, types of user roles associated with test cases, facility defined versus developer defined test cases).

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

## Recommended Practice

**1.5** Clinical applications and system interfaces are tested individually and as-installed before go-live and are closely monitored after go-live.[16]

*Checklist*

## Implementation Status

## Rationale for Practice or Risk Assessment

Safety events can result from 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.[14]
- System-system interfaces between key clinical applications (e.g., CPOE and pharmacy, 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.[17]

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

## Recommended Practice

**1.6** Computers and displays in publicly accessible areas are configured to ensure that patient identifiable data are physically and electronically protected.[18]

*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 at 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, 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, backups are kept in a different location).
- All portable computing devices used to access EHR data have encrypted hard drives.[19]
- Backups containing patient-identifiable data are encrypted.

## Recommended Practice

**1.7** There are processes in place to ensure data integrity during and after major system changes, such as upgrades to hardware, operating systems, or browsers.[20]
*Checklist*

## Implementation Status

## 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 not acceptable.

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 change management and internal control policies and procedures to ensure data integrity, and these 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:[21]
  - 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)
- Standard, regularly used clinical and administrative reports (e.g., length of stay, readmission rates, alert override rates) are generated and reviewed periodically to ensure that the data on which they are based has not changed in a way that renders the report meaningless. When changes in underlying data have the potential to lead to faulty conclusions, users are notified as soon as possible, and repairs are implemented in a timely manner.
- If data becomes corrupted, the organization has policies and processes for reverting to a backup version of the data that precedes the corruption. In addition, there are policies and processes for:
  - Integrity checks to ensure a successful recovery after reverting to the backup
  - Downtime processes to ensure access to critical data while the system is brought back to an uncorrupted state
  - Methods for re-entry of data generated (e.g., orders, notes) during the period of system corruption and subsequent downtime

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

## Recommended Practice

**2.1** 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.[22]

*Checklist*

## Implementation Status

## 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 the accuracy and timeliness of information display and entry.

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, “canned text”).[23]
- Default values are available for common orders (e.g., medication order sentences, 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.[24]

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

## Recommended Practice

**2.2** 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.[4]
*Checklist*

## Implementation Status

## 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.[4]

## Recommended Practice

**2.3** 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.[25]

*Checklist*

## Implementation Status

## 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 and training 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.[26]
- The EHR is configured to make it difficult to confuse the live version of the EHR with other versions (e.g., 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 include numbers in the name.[14]
- Use of generic accounts in the production environment (e.g., "MD-Test" used by HIT support staff and others for role-based testing) are tightly controlled (e.g., with regular password changes, restricted admin-level rights, regular review of real patient data that were accessed).

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

## Recommended Practice

**2.4** System configuration settings that limit clinicians in their practice are minimized, carefully implemented following clinician acceptance, and closely monitored.[27]

*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

- EHR change/configuration management related organizational policies and procedures that address decisions to limit clinicians in their practice (e.g., mandatory clinical alert settings, hard stops that cannot be overridden by clinicians, alerts that cannot be turned off by clinicians) are developed with clinician input, judiciously implemented, and carefully monitored.[28]
- Organizational policy and procedures minimize configurations that limit clinicians' ability to continue practicing (e.g., enter new orders) due to incomplete work (e.g., overdue co-signatures, incomplete discharge summaries).

## Recommended Practice

## Implementation Status

**2.5** The human-computer interface is configured for optimal usability for different users and clinical contexts.[29]

*Checklist*

### 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 (i.e., 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, or display fields, are set wide enough to see key data.[16]
- 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.

## Recommended Practice

**3.1** The organization has processes and methods in place to monitor the effects of key configuration settings to ensure they are working as intended.[30]

*Checklist*

## Implementation Status

## Rationale for Practice or Risk Assessment

Failure to monitor configuration settings associated with key clinical components (e.g., CPOE interface to pharmacy) or 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. The organization has 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.[31]
- 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.[32]
- Clinical decision support is monitored using statistical processes (e.g., control charts) to identify malfunctions.[33]

## References

1. Howard, J., Clark, E. C., Friedman, A., Crosson, J. C., Pellerano, M., Crabtree, B. F., ... & Cohen, D. J. (2013). Electronic health record impact on work burden in small, unaffiliated, community-based primary care practices. Journal of General Internal Medicine, 28(1), 107-113.

2. Sittig, D. F., Campbell, E. M., Guappone, K. P., Dykstra, R. H., & Ash, J. S. (2007). Recommendations for monitoring and evaluation of in-patient computer-based provider order entry systems: results of a Delphi survey. American Medical Informatics Association Annual Symposium Proceedings, 2007, 671–675.

3. Haskins, M. (2002). Legible charts! Experiences in converting to electronic medical records. Canadian Family Physician, 48, 768.

4. Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: a systematic literature review. Journal of Biomedical Informatics, 46(3), 541-562.

5. Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2015). Enterprise Cybersecurity Capabilities. In Enterprise Cybersecurity (pp. 311-334). Apress.

6. O'Connor, K. J. (2005). Everything you always wanted to know about software escrow agreements--and then some! Journal of Healthcare Information Management, 19(1), 10.

7. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583-592.

8. Tipton, S. J., Forkey, S., & Choi, Y. B. (2016). Toward proper authentication methods in electronic medical record access compliant to HIPAA and CIA triangle. Journal of Medical Systems, 40(4), 1-8.

9. Sasse, M. A. (2013, August). “Technology Should Be Smarter Than This!”: A Vision for Overcoming the Great Authentication Fatigue. Workshop on Secure Data Management (pp. 33-36). Springer International Publishing.

10. Clayton, P. D., Boebert, W. E., Defriese, G. H., Dowell, S. P., Fennell, M. L., Frawley, K. A., ... & Rindfleisch, T. C. (1997). For the record: protecting electronic health information. National Research Council. (Washington, DC: National Academy Press, 1997).

11. Cresswell, K. M., Mozaffar, H., Lee, L., Williams, R., & Sheikh, A. (2016). Safety risks associated with the lack of integration and interfacing of hospital health information technologies: a qualitative study of hospital electronic prescribing systems in England. BMJ Quality & Safety.

12. Berger, R. G., & Baba, J. (2009). The realities of implementation of Clinical Context Object Workgroup (CCOW) standards for integration of vendor disparate clinical software in a large medical center. International Journal of Medical Informatics, 78(6), 386-390.

13. Ancker, J. S., Singh, M. P., Thomas, R., Edwards, A., Snyder, A., Kashyap, A., & Kaushal, R. (2013). Predictors of success for electronic health record implementation in small physician practices. Applied Clinical Informatics,4(1), 12-24.

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

15. Frankel, A., Grillo, S. P., Baker, E. G., Huber, C. N., Abookire, S., Grenham, M., ... & Gandhi, T. K. (2005). Patient safety leadership WalkRounds™ at Partners HealthCare: learning from implementation. The Joint Commission Journal on Quality and Patient Safety, 31(8), 423-437.

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

17. Li, A. C., Kannry, J. L., Kushniruk, A., Chrimes, D., McGinn, T. G., Edonyabo, D., & Mann, D. M. (2012). Integrating usability testing and think-aloud protocol analysis with “near-live” clinical simulations in evaluating clinical decision support. International Journal of Medical Informatics, 81(11), 761-772.

18. Murphy, A. R., Reddy, M. C., & Xu, H. (2014, February). Privacy practices in collaborative environments: a study of emergency department staff. Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing (pp. 269-282). ACM.

19. Benusa, A., & Chen, J. (2015). HIPAA compliance challenges: a case study of a small healthcare provider. Proceedings of the 5th International Conference on IS Management and Evaluation 2015: ICIME 2015 (p. 161). Academic Conferences Limited.

20. Nelson, R., & Staggers, N. (2014). Health informatics: an interprofessional approach. Elsevier Health Sciences.

21. Pageler, N. M., G’Sell, M. J. G., Chandler, W., Mailes, E., Yang, C., & Longhurst, C. A. (2016). A rational approach to legacy data validation when transitioning between electronic health record systems. Journal of the American Medical Informatics Association.

## References

22. Ash, J. S., Sittig, D. F., Guappone, K. P., Dykstra, R. H., Richardson, J., Wright, A., ... & Middleton, B. (2012). Recommended practices for computerized clinical decision support and knowledge management in community settings: a qualitative study. BMC Medical Informatics and Decision Making, 12(1), 1.

23. Bobb, A. M., Payne, T. H., & Gross, P. A. (2007). Viewpoint: controversies surrounding use of order sets for clinical decision support in computerized provider order entry. Journal of the American Medical Informatics Association, 14(1), 41-47.

24. Wright, A., Ash, J. S., Erickson, J. L., Wasserman, J., Bunce, A., Stanescu, A., ... & Middleton, B. (2014). A qualitative study of the activities performed by people involved in clinical decision support: recommended practices for success. Journal of the American Medical Informatics Association, 21(3), 464-472.

25. 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.

26. Lincke, S. (2015). Designing Information Security. In Security Planning (pp. 115-133). Springer International Publishing.

27. Eikey, E. V., Murphy, A. R., Reddy, M. C., & Xu, H. (2015). Designing for privacy management in hospitals: understanding the gap between user activities and IT staff's understandings. International Journal of Medical Informatics, 84(12), 1065-1075.

28. Strom, B. L., Schinnar, R., Aberra, F., Bilker, W., Hennessy, S., Leonard, C. E., & Pifer, E. (2010). Unintended effects of a computerized physician order entry nearly hard-stop alert to prevent a drug interaction: a randomized controlled trial. Archives of Internal Medicine, 170(17), 1578-1583.

29. Middleton, B., Bloomrosen, M., Dente, M. A., Hashmat, B., Koppel, R., Overhage, J. M., ... & Zhang, J. (2013). Enhancing patient safety and quality of care by improving the usability of electronic health record systems: recommendations from AMIA. Journal of the American Medical Informatics Association, 20(e1), e2-e8.

30. Meeks, D. W., Takian, A., Sittig, D. F., Singh, H., & Barber, N. (2014). Exploring the sociotechnical intersection of patient safety and electronic health record implementation. Journal of the American Medical Informatics Association, 21(e1), e28-e34.

31. Smith, M. W., Ash, J. S., Sittig, D. F., & Singh, H. (2014). Resilient practices in maintaining safety of health information technologies. Journal of Cognitive Engineering and Decision Making, 8(3), 265-282.

32. McCoy, A. B., Waitman, L. R., Lewis, J. B., Wright, J. A., Choma, D. P., Miller, R. A., & Peterson, J. F. (2012). A framework for evaluating the appropriateness of clinical decision support alerts and responses. Journal of the American Medical Informatics Association, 19(3), 346-352.

33. Wright, A., Hickman, T. T. T., McEvoy, D., Aaron, S., Ai, A., Andersen, J. M., ... & Bates, D. W. (2016). Analysis of clinical decision support system malfunctions: a case series and survey. Journal of the American Medical Informatics Association.