



JCI Accreditation Standards for Hospitals and Academic Medical Centers (AMC), 8th Edition

Draft Standards for Field Review Proposed New Standards and Requirements

Note: This document does not include all standards for Hospitals and Academic Medical Centers (AMC), 8th Edition. The standards in this document are the proposed requirements in the Management of Information (MOI) and Health Care Technology (HCT) chapters only. To participate in the field review of other chapters of the hospital and AMC standards, please refer back to the JCI website.

While the HCT chapter is new, not all standards are new. Some standards in the HCT chapter were taken from other existing chapters to consolidate related topics on new and emerging methods of health care technology from electronic health records (EHR) to telehealth capabilities, artificial intelligence, medical equipment advancements, technological innovations.

As a reminder, the field review focuses on newly added or significantly revised requirements. To identify the difference:

- Standards, measurable elements, intents, and guidance that are new or have undergone significant changes that have impacted the intent of the requirement are in **RED font**.
- Standards, measurable elements, intents, and guidance that are in **BLACK font** may have undergone changes, but the intents remained the same.

Prior to the publication, a complete summary of changes will be included in the manual along with an updated and complete reference list for each chapter.

Field Review Questionnaire: To participate in the field review of this chapter, please complete the survey below:

<https://www.surveymonkey.com/r/ZTD36H5>

Field Review Period: **October 23- November 13, 2023**

**CONFIDENTIAL PROPOSED REQUIREMENTS FOR FIELD REVIEW PURPOSE ONLY
DO NOT COPY – DO NOT DISTRIBUTE**

Management of Information (MOI)

Overview

Providing patient care is a complex endeavor that is highly dependent on the communication of information. This communication is to and with patients and their families, other health care practitioners, and the community. Failures in communication are one of the most common root causes of patient safety incidents. Often, these communication failures result from illegible handwriting, and the nonuniform or non-standardized use of abbreviations, symbols, and codes across an organization. An integral part of information management in health care is monitoring and protecting the use of patients' information. To provide, coordinate, and integrate services, health care organizations rely on information about the science of care, individual patients, care provided, results of care, and their own performance. Like human, material, and financial resources, information is a resource that must be managed effectively by the organization's leaders. Every organization seeks to obtain, to manage, and to use information to improve patient outcomes as well as individual and overall organization performance.

Over time, organizations become more effective in

- identifying information and information technology needs;
- designing/deploying information management systems;
- defining and capturing data and information;
- analyzing data and transforming it into information;
- transmitting and reporting data and information;
- protecting confidentiality, security, and integrity of data and information; and
- integrating and using information for performance improvement.

Although computerization and other technologies improve efficiency, the principles of good information technology management apply to all documentation methodologies. These standards are designed to be equally compatible with noncomputerized systems and current/future technologies.

Standards

The following is a list of all standards for this function. They are presented here for your convenience without their intent statements or measurable elements. For more information about these standards, please see the next section in this chapter, Standards, Intent, Guidance, and Measurable Elements.

Information Management

- MOI.1 The hospital plans for managing information and selects processes to meet the needs of those who require data and information.
- MOI.2 The hospital maintains the confidentiality, security, privacy, and integrity of data and information through processes to manage and control access.
- MOI.2.1 The hospital maintains the confidentiality, security, privacy, and integrity of data and information through processes that protect against loss, theft, damage, destruction, ransomware, and other cyber-attacks.
- MOI.3 The hospital determines the retention time of patient medical records, data, and other information.
- MOI.4 The hospital uses standardized diagnosis and procedure codes and ensures the uniform use of approved symbols and abbreviations across the hospital.
- MOI.5 The hospital retrieves, disseminates, and transmits health information on a timely basis in a format that meets user expectations, and with the desired frequency.
- MOI.6 Clinical staff, decision makers, and other staff members are educated and trained on information systems, information security, and the principles of information use and management.

Management and Implementation of Documents

MOI.7 Documents, including policies, procedures, and programs, are managed in a consistent and uniform manner.

MOI.7.1 Leaders review, approve, and manage implementation of policies and procedures that guide and support patient care and services.

Patient Medical Record

MOI.8 The hospital initiates and maintains a standardized, accurate medical record for every patient assessed or treated and determines the record's content, format, and location of entries.

MOI.9 As part of its monitoring and performance improvement activities, the hospital regularly assesses patient health record content.

Information Technology in Health Care

MOI.10 Hospital leadership identifies a qualified individual to oversee the hospital's health information systems and processes.

MOI.11 The hospital develops, maintains, and tests a program for response to planned and unplanned downtime of data systems.

MOI.12 The hospital develops and maintains processes and procedures for cybersecurity and cyber risk management.

Standards, Intents, Guidance, and Measurable Elements

Information Management

Standard MOI.1

The hospital plans for managing information and selects processes to meet the needs of those who require data and information.

Intent of MOI.1

Information is generated and used during patient care, treatment, and services and for managing a safe and effective hospital.

Guidance for MOI.1

The ability to capture and to provide information requires effective planning. Planning for information management may include:

- The hospital's mission
- Services provided
- Resources
- Access to affordable technology
- Usability and interoperability assessments
- Support for effective communication among caregivers.

Planning incorporates input from a variety of sources who use data and information, including the following:

- Health care practitioners and other staff who provide clinical services
- Hospital leaders and department/service leaders
- Individuals, services, and agencies outside the hospital who use data or information about the hospital's operation and care processes

The information needs of these sources should inform the hospital's information management strategies and ability to implement those strategies. The strategies must meet the needs of the hospital based on the hospital's size, complexity of services, availability of trained staff, and other human and technical resources.

The information processes are comprehensive and include all of the departments and services of the hospital. Planning for the management of information does not require a formal written information program but does require evidence of a planned approach that identifies the hospital's information needs and processes for meeting those needs.

Measurable Elements of MOI.1

- ❑ 1. The hospital plans and implements processes to meet the information needs of
 - a) Those who provide clinical services
 - b) The hospital's leaders and department/service leaders
 - c) Individuals, services, and agencies outside the hospital
 - d) Patients accessing personal data
- ❑ 2. The processes implemented are appropriate to the hospital's size, complexity of services, availability of trained staff, technical resources, and other resources.
- ❑ 3. The planning and designing of information management processes to meet the information needs of the hospital include:
 - a) The hospital's mission
 - b) Services provided
 - c) Resources
 - d) Access to affordable technology
 - e) Usability and interoperability assessments
 - f) Support for effective communication among caregivers

Standard MOI.2

The hospital maintains the confidentiality, security, privacy, and integrity of data and information through processes to manage and control access.

Intent of MOI.2

The hospital establishes processes to protect sensitive patient information and prevent unauthorized access to data which can have larger consequences.

Guidance for MOI.2

The balance between data sharing and data confidentiality is addressed. The hospital should follow established processes for the safe movement within and release of patient health record information.

Whether a hospital uses paper and/or electronic information systems, the hospital implements measures to secure and protect data and information at all times. Data and information include:

- Patient health records
- Data from medical equipment and devices
- Research data
- Quality data
- Billing data
- Human resources data
- Other applicable sources

Security measures include processes to manage and control access. The hospital determines who is authorized to access health records and implements processes for assigning privileges to authorized users in accordance with their level of access. An authorized user may be able to enter, modify, and delete information, or may have read-only or restricted access to some systems or modules. Level of access may identify who can make entries in the health record, who can enter patient orders, who can access high-security patient cases, who can access quality improvement data, and so on.

For hospitals with electronic information systems, monitoring access to patient data and information through security audits of access logs can help protect confidentiality and security. The hospital implements regular security audits to proactively monitor access logs and identify system vulnerabilities or confidentiality policy violations.

CONFIDENTIAL PROPOSED REQUIREMENTS FOR FIELD REVIEW PURPOSE ONLY
DO NOT COPY – DO NOT DISTRIBUTE

Hospitals that use documentation assistants, or scribes, have a process to ensure protection of patient information including training, competencies, stated job responsibilities, and a clearly identified scope of documentation activity. When electronic health records are used, additional security measures are implemented (**for example**, unique credentials assigned only to them).

Each authorized individual's level of access to data and information is based on need and defined by the person's role and responsibilities. Students, trainees, scribes, and others, as determined by the hospital, are included. An effective process defines

- Who is authorized to have access to data and information, including patient health records
- The information to which an authorized individual has access (level of access)
- The process for granting access privileges to authorized individuals
- The individual's obligation to keep information confidential and secure
- The process for maintaining data integrity (accuracy, consistency, and completeness)
- The process followed when confidentiality, security, or data integrity are violated or compromised

Security audits can identify system users who have altered, edited, or deleted information and can track changes made to the electronic health record. This information can be used to

- Validate user permissions are set appropriately according to current roles
- Identify user permissions that need to be removed due to staff changes

If a hospital is planning to transition from a physical to an electronic health record system, considerations must be made to ensure the safety and confidentiality of patient information. Factors to consider include

- Timeframe for conversion of data
- Which information needs to be converted
- Destroying data no longer necessary
- How the information will be converted (**for example**, direct data entry or scanning)
- Where the data entry occurs (**for example**, centralized or decentralized)

Measurable Elements of MOI.2

- 1. The hospital implements processes consistent with laws and regulations to ensure the confidentiality, security, and integrity of data and information.
- 2. The hospital identifies those authorized to access data and information, including those authorized to make entries in the patient health record, and determines their level of access based on each individual's role and responsibilities.
- 3. The hospital has a process in place to grant authorized individuals access privileges to data and information in accordance with their level of access.
- 4. The hospital implements processes to ensure that data and information are accessed by authorized individuals only and in accordance with their level of access.
- 5. The hospital implements processes to ensure that only authorized individuals make entries in the patient health record and in accordance with their level of access.
- 6. The hospital monitors compliance with the processes and release of information and acts when violations occur.

Standard MOI.2.1

The hospital maintains the confidentiality, security, privacy, and integrity of data and information through processes that protect against loss, theft, damage, destruction, ransomware, and other cyber-attacks.

Intent of MOI.2.1

Vulnerabilities that lead to the breach of sensitive information and data can be severe and widespread for the hospital and the patients it serves.

Guidance for MOI.2.1

The hospital ensures that paper and electronic health records, data, and other information are protected from loss, theft, tampering, damage, and unintended destruction.

CONFIDENTIAL PROPOSED REQUIREMENTS FOR FIELD REVIEW PURPOSE ONLY
DO NOT COPY – DO NOT DISTRIBUTE

Vulnerabilities that pose a security risk include response to phishing emails, sending unencrypted emails, password misuse, or misplaced technological equipment. The hospital also assesses for external/remote cybersecurity vulnerabilities including hacking, breach of information, ransomware or other malware.

To protect data and information, the hospital implements best practices for data security and ensures safe and secure storage of health records, data, and information. **Examples** of security measures and strategies include, but are not limited to, the following:

- Ensuring that security software and system updates are current and up to-date
- Encrypting data, such as data stored in digital form
- Protecting data and information through backup strategies such as off-site storage and/or cloud backup services
- Storing physical health records in locations where they will be protected from heat, water, fire, pests, or infestation
- Storing active health records in areas where only authorized health care practitioners have access
- Ensuring that server rooms and areas where physical health records are stored are secured and only accessible by authorized individuals
- Ensuring that server rooms and areas where physical health records are kept at proper temperature and humidity levels to protect servers/records
- Ensuring that server rooms and areas where physical health records are kept are protected from fire hazards
- Conducting and documenting an ongoing information security risk assessment, at least annually.

A risk assessment considers a review of processes and new and planned services that may pose risks to data and information. Risks are prioritized from the risk assessment, and improvements are identified and implemented to address the risks. Improvements are monitored to ensure that risks are prevented or eliminated.

Technology advancements create increased opportunities for electronic information to be breached. The hospital ensures staff are trained, at least annually, in topics including the following:

- Log-in processes and behaviors (for example, not sharing credentials)
- Malware training
- Email phishing reporting

Measurable Elements of MOI.2.1

- 1. The hospital conducts and documents an annual information security risk assessment throughout the organization, and data security risks are identified and prioritized from the risk assessment.
 - 2. Data and information are stored in a manner that protects against loss, theft, damage, destruction, ransomware and other cyber-attacks.
 - 3. The hospital implements data security best practices to protect and secure data and information.
 - 4. The hospital identifies goals, implements improvements to address data security risks, and monitors improvement data to ensure that risks are reduced or eliminated.
-

Standard MOI.3

The hospital determines the retention time of patient health records, data, and other information.

Intent of MOI.3

The hospital determines the retention time of health records, data, and other information that are retained for sufficient periods to comply with laws and regulations and to support patient care, management, legal documentation, research, and education as applicable.

Guidance for MOI.3

The retention process for health records, data, and other information, including text messages and e-mails that contain information for health records, is consistent with the hospital policies and procedures for maintaining the confidentiality and security of such

CONFIDENTIAL PROPOSED REQUIREMENTS FOR FIELD REVIEW PURPOSE ONLY
DO NOT COPY – DO NOT DISTRIBUTE

information. After the retention period, patient health records, data, and other information are destroyed in a manner that does not compromise confidentiality and security.

Measurable Elements of MOI.3

- 1. The hospital determines the retention time of patient health records and other data and information and complies with laws and regulations.
 - 2. The retention process provides expected confidentiality and security.
 - 3. Patient health records, data, and other information are destroyed or deleted in a manner that does not compromise confidentiality and security.
-

Standard MOI.4

The hospital uses standardized diagnosis and procedure codes and ensures the uniform use of approved symbols and abbreviations across the hospital.

Intent of MOI.4

Standardization of codes and uniform use of symbols and abbreviations prevents miscommunication and potential errors in patient care and supports data aggregation and analysis.

Guidance for MOI.4

Abbreviations can be problematic and even dangerous, particularly in the context of prescribing medications. When abbreviations are allowed in the hospital, processes are implemented to prevent or reduce risks to patient safety. Abbreviations are not used on high risk, patient-specific documents that are crucial to continuity of care including

- Informed consent documents
- Patient rights documents
- Discharge instructions
- Discharge summaries

Patients and families may not understand the hospital's approved abbreviations. With discharge summaries, there is a patient safety risk in using abbreviations if a provider from a different organization does not use the same list. Abbreviations are typically used on reports of laboratory and diagnostic imaging test results.

The hospital's use of standardized codes and uniform use of approved symbols and abbreviations is consistent with standards of professional practice and complies with local laws and regulations as applicable. Staff are educated and trained on the principles of the standardization and uniform use of the hospital's codes, symbols, and abbreviations.

When a hospital uses abbreviations, the hospital implements a process for the uniform use of approved abbreviations, such as a reference list. This uniform use includes each abbreviation having only one meaning. When abbreviations have more than one meaning, confusion as to what the author meant may result in medical errors. **For example**, the abbreviation *MS* could mean mitral stenosis in cardiology; however, in neurology, the abbreviation *MS* may be used for multiple sclerosis. In addition, confusion may arise when two abbreviations have the same letters but different letter cases. **For example**, *Pt* for patient and *PT* for physiotherapy. Even though the use of uppercase and lowercase letters differs between the two **examples**, they are essentially the same abbreviation with more than one meaning. It is important that abbreviation use is uniform and consistent across the hospital without differences in meanings between different departments or services.

When a hospital uses abbreviations, the hospital develops and/or adopts a do-not-use list of abbreviations and symbols. **For example**, the Institute for Safe Medication Practices (ISMP) maintains a list of abbreviations, symbols, and dose designations that "should never be used when communicating medical information." The items in the list were reported to ISMP as being frequently misinterpreted and involved in harmful medication errors.

If abbreviations are necessary in a high-risk document, the first occurrence of the term should be completely spelled out with the abbreviation listed in parentheses.

Measurable Elements of MOI.4

- 1. The hospital uses standardized diagnosis codes and procedure codes.
- 2. The hospital implements the uniform use of approved symbols and identifies those not to be used.
- 3. If the hospital allows abbreviations, it meets the following criteria
 - a. The hospital implements a uniform use of approved abbreviations with only one meaning
 - b. The hospital implements a do-not-use list of abbreviations
 - c. The hospital does not use abbreviations on informed consents, patient rights documents, discharge instructions, or discharge summaries
 - d. When an abbreviation is first used in documentation, the term must first be spelled out in complete form with the abbreviation in parentheses
 - e. The hospital monitors use of abbreviations and takes action to improve processes as needed

Standard MOI.5

The hospital retrieves, disseminates, and transmits health information on a timely basis in a format that meets user expectations, and with the desired frequency.

Intent of MOI.5

The dissemination of data and information to meet the needs of those in and outside the hospital is an important aspect of information management.

Guidance for MOI.5

Internally, health care practitioners, hospital leaders, department/service leaders, and other staff require specific data and information in a timely manner to allow them to carry out their responsibilities effectively and efficiently. **For example**, health care practitioners caring for a patient, including physicians, nurses, dietitians, pharmacists, and others, need access to up-to-date information and all applicable sections of the patient's medical record to provide safe and effective patient care.

Externally, the hospital may provide data and information to regulatory agencies (such as the Ministry of Health), health care practitioners (such as a patient's primary care physician in the community), health care services and programs (such as an outside laboratory or an organization for patient referral), and individuals (such as patients who request their medical record after discharge from the hospital).

The format and time frame for disseminating data and information are tailored to meet the user's expectations of the individual, service, or program. When data and information are needed for the care of a patient, it is provided in a timely manner that supports continuity of care and patient safety.

Examples of dissemination strategies to meet user expectations include

- providing the specific data and information requested/required;
- providing reports with the frequency needed by the individual or program;
- providing data and information in a format that facilitates its use;
- linking sources of data and information; and
- providing interpretation or clarification of data.

Measurable Elements of MOI.5

- 1. Data and information dissemination meets the needs of individuals and programs within and outside the hospital that provide patient care, treatment, and services.
- 2. The hospital disseminates data and information in useful formats within time frames that are defined by the hospital and consistent with law and regulation.
- 3. Staff providing patient care have access to the data and information needed to carry out their job responsibilities and provide patient care safely and effectively.

Standard MOI.6

Clinical staff, decision makers, and other staff members are educated and trained on information systems, information security, and the principles of information use and management.

Intent of MOI.6

Individuals in the hospital who generate, collect, enter, review, analyze, and use data and information are educated and trained to effectively perform their job functions.

Guidance for MOI.6

This education and training enables these individuals to

- use information systems, such as an electronic health record system, to carry out their job responsibilities efficiently and safely
- comply with policies and procedures to ensure security and confidentiality of data and information
- implement tactics and strategies for the management of data, information, and documentation during planned and unplanned downtime
- use data and information to help in decision making
- educate and support patients and families regarding participation in care processes
- use measures to assess and improve care and work processes

Hospitals with electronic health record systems ensure that staff who need to access, review, and/or document in the patient health record receive education, ongoing training, and assessment to effectively and efficiently use the system.

Cybersecurity breaches can pose safety issues for patients and be costly to the hospital system. Hospitals also ensure staff receive cybersecurity training related to their responsibilities and job descriptions to maintain security of information.

The information management process makes it possible to combine information from various sources and generate reports to support decision making with longitudinal and comparative data. The combination of clinical and managerial information helps department/service leaders to plan collaboratively.

Various methods can be used for ongoing training that are relevant to staff needs and provide helpful guidance on system use. **For example**

- “Tips and tricks”
- Quick reference guides
- Short educational modules
- Newsletters can be posted or e-mailed

Cybersecurity education and training topics can include

- Password protection
- Malware and ransomware
- Email phishing
- Device management
- Safeguards for sensitive data
- Device updates
- Reporting suspicious activity

Measurable Elements of MOI.6

1. Clinical staff, decision makers, and others are provided education and training on information systems, information security, and the principles of information use and management, as appropriate to their role and responsibilities.

**CONFIDENTIAL PROPOSED REQUIREMENTS FOR FIELD REVIEW PURPOSE ONLY
DO NOT COPY – DO NOT DISTRIBUTE**

- 2. Staff who use an electronic health record system receive education, ongoing training, and assessment to ensure that they can effectively and efficiently use the system to carry out their job responsibilities.
- 3. Staff receive education and ongoing training related to cybersecurity based on their roles and responsibilities
- 4. Clinical and managerial data and information are integrated as needed to support decision making.

Management and Implementation of Documents

Standard MOI.7

Documents, including policies, procedures, and programs, are managed in a consistent and uniform manner.

Intent of MOI.7

Policies and procedures are intended to provide uniform knowledge on organizational clinical and nonclinical functions.

Guidance for MOI.7

A written document guides how all policies, procedures, and programs in the hospital will be developed and controlled.


Measurable Elements of MOI.7

- 1. There is a written guidance document that defines the requirements for reviewing policies and procedures including
 - a) Review and approval of all documents by an authorized person before issue
 - b) Frequency of review and continued approval of documents
 - c) Controls for ensuring that only current, relevant versions of documents are available
 - d) Method for identifying changes
- 2. There is a written guidance document that defines requirements for management of policies and procedures including
 - a) Maintaining identity and legibility
 - b) Managing documents originating outside the hospital
 - c) Retaining obsolete documents for the time required by laws and regulations while ensuring they are not used
 - d) Tracking all documents in circulation (for example, identified by title, date of issue, edition and/or current revision date, number of pages, and who authorized and/or reviewed the document)
- 3. There are standardized formats for all similar documents; **for example**, all policies.
- 4. The requirements of the guidance document are implemented and evident in the policies, procedures, and programs found throughout the hospital.

Standard MOI.7.1

Leaders review, approve, and manage implementation of policies and procedures that guide and support patient care and services.

Intent of MOI.7.1

Throughout the accreditation standards found in this manual, policies, procedures, plans, and other written documents are required (noted with the icon ) , as they reduce process variation and reduce the risk inherent in processes to improve quality and patient safety.

Guidance for MOI.7.1

**CONFIDENTIAL PROPOSED REQUIREMENTS FOR FIELD REVIEW PURPOSE ONLY
DO NOT COPY – DO NOT DISTRIBUTE**

There is a process to ensure that staff members have read and are familiar with policies, procedures, and plans relevant to their work. This process may be part of the orientation of staff members to their department and responsibilities or may be part of groupwide or hospital wide special training sessions. When a policy, procedure, or plan is relevant to the assignment of an individual, the intended actions described in the document are evident in the actions of the individual.

Measurable Elements of MOI.7.1

- 1. Required policies, procedures, and plans are available, and staff understand how to access those documents relevant to their responsibilities.
 - 2. Staff are trained and understand those documents relevant to their responsibilities.
 - 3. The requirements of the policies, procedures, and plans are fully implemented and evident in the actions of individual staff members.
 - 4. The implementation of policies, procedures, and plans is monitored, and the information supports full implementation.
-

Patient Health Record

Standard MOI.8

The hospital initiates and maintains a standardized, accurate health record for every patient assessed or treated and determines the record's content, format, and location of entries.

Intent of MOI.8

The integrity of the patient health record is critical to the quality, safety, and continuity of care, as it is the principal tool for communication between health care practitioners.

Guidance for MOI.8

Every patient assessed or treated in the hospital has a single health record that is assigned with unique identifiers, or some other mechanism used to link the patient with their health record. The unique identifiers used in health records are uniform throughout the hospital to ensure ease of locating and documenting on care of patients.

Processes ensure that each entry in the patient health record identifies the author, the date, and the time of entries, such as for timed treatments and medication orders. There is also a process for how entries in a health record are corrected or overwritten. This applies to any physician, practitioner, or documentation assistant.

Electronic functions in documentation by practitioners is becoming more common practice as electronic health records systems are being adopted. These can include

- Copy-and-paste (the practice of selecting text or data from an original or previous source to reuse in a different location)
- Templates
- Auto-fill
- Auto correct

Electronic functions can have advantages, but also pose safety risks of inaccuracy or duplication of information. **For example,**

- A health care practitioner may copy his or her own notes to reuse, copy a note from another practitioner, or copy from a prior admission without updating appropriately.
- A template used for an emergency examination may include data fields for all body systems. When a focused examination is completed, documentation in the template may indicate that a complete examination was performed and was within normal limits. If an examination did not occur, but is documented as normal, patients and health care practitioners may make treatment decisions based on this misinformation.

Hospitals implement processes to ensure the accuracy of data and information in patient health records, including guidelines for the proper use of copy-and-paste, auto-fill, auto-correct, and templates in the electronic health record, as well as monitoring their use.

Hospitals also provide training and education on the proper use of electronic documentation functions to all staff who document in the health record.

When both an electronic and hard copy of health records are actively in use, hospitals implement processes to ensure consistency of information between sources. The primary health record, whichever source, should be comprehensive and should not have missing information from the other source. Duplication of information should be avoided to accuracy of the health record.

Identifiers for patient health records can include a combination of

- The health record number
- The patient's name
- The patient's date of birth

The content, format, and location of entries for a patient's health record is standardized to help promote the integration among health care practitioners and continuity of care. The hospital determines the specific data and information recorded in the health record of each patient assessed or treated including

- Patient demographics
- Medications
- Patient diagnoses/problem list
- Assessment/reassessment
- Testing results
- Care plan
- Health maintenance

The health record needs to present sufficient information to

- Support the diagnosis
- Justify the patient's care, treatment, and services
- Document the course and results of the patient's care, treatment, and services
- Facilitate the continuity of care.

Monitoring electronic function use in documentation may involve partnering with the electronic health record vendor to develop a way to track information that has been copied-and-pasted or auto-generated (**for example,** displaying this information in a different font or underlined) or using a manual process to review for copied-and-pasted information.

Measurable Elements of MOI.8

- 1. The patient health record contains
 - a) At least two unique identifiers
 - b) The author of each entry
 - c) The date of each entry
 - d) The time of each entry
- 2. The specific content, format, and location of entries for patient health records is standardized and determined by the hospital.
- 3. The hospital implements a process on the proper use of copy-and-paste, auto-fill, auto-correct, and templates and provides education and training on the process to all staff who document in the electronic health record.
- 4. The hospital implements processes to facilitate accurate and complete documentation in patient health records.
- 5. There are processes for how entries are corrected, overwritten, reviewed, and authenticated.

CONFIDENTIAL PROPOSED REQUIREMENTS FOR FIELD REVIEW PURPOSE ONLY
DO NOT COPY – DO NOT DISTRIBUTE

Standard MOI.9

As part of its monitoring and performance improvement activities, the hospital regularly assesses patient health record content.

Intent of MOI.9

Each hospital determines the content and format of the patient health record and has a process to assess the content and completeness as part of the hospital's performance improvement activities and is carried out regularly.

Guidance for MOI.9

Patient health record review is based on a sample representing the practitioners providing care and the types of care provided. The review process is conducted by medical staff, nursing staff, and other relevant health care practitioners who are authorized to make entries in the patient health record. The review focuses on the timeliness, accuracy, completeness, and legibility of the record and clinical information. Health record content required by laws or regulations is included in the review process. The hospital's health record review process includes health records of all services provided to both current and discharged patients.

A representative sample means health records from all services and not a specific sample size; however, it should make sense for the organization.

Measurable Elements of MOI.9

- 1. A representative sample of health records that includes active and discharged health records in all service areas, is reviewed at least quarterly or more frequently as determined by laws and regulations.
- 2. The review is conducted by physicians, nurses, and others authorized to manage or make entries in patient health records.
- 3. The review focuses on the timeliness, accuracy, completeness, and legibility of the health record.
- 4. Health record content required by laws or regulations is included in the review process.
- 5. The results of the review process are incorporated into the hospital's quality oversight mechanism.

Information Technology in Health Care

Standard MOI.10

Hospital leadership identifies a qualified individual to oversee the hospital's health information systems and processes.

Intent of MOI.10

Successful implementation of new and evolving health information systems requires support, resources, and direction from hospital leadership.

Guidance for MOI.10

Leadership identifies a qualified individual to oversee health information systems in the organization. The individual is qualified by education, training, and/or experience relevant to the role and responsibilities. Depending on the size and scope of the hospital's information systems, there may be several individuals who support this individual and help manage aspects of the program.

The hospital's information systems must be managed effectively and in a comprehensive and coordinated manner. The individual who oversees the health information systems is responsible for at least the following:

- Coordinating and conducting risk assessment activities to assess information security risks, prioritize risks, and identify improvements
- Ensuring that staff and others are educated and trained on information security and applicable policies and procedures

- Identifying metrics to assess how systems, such as the electronic health record system, are functioning and affecting staff and patients

Health information systems interact with processes within the hospital, other organizations outside of the hospital, and internal and external health care practitioners, as well as patients and families. This level of complex integration requires coordinated participation from key stakeholders. Under the leadership of the individual who oversees health information systems in the hospital, stakeholders, such as clinical and nonclinical staff and department/service leaders, are involved in workflow analysis, the selection process for new systems, and their testing, implementation, and evaluation. Analysis of workflow processes prior to and after selection and implementation will help assess how systems can be optimized and modified when necessary.

Measurable Elements of MOI.10

- 1. Hospital leadership provides direction, support, and resources for health information systems in the hospital.
- 2. Hospital leadership identifies a qualified individual to oversee health information systems in the hospital
- 3. **A qualified individual conducts and documents an annual risk assessment of the health information systems.**
- 4. Stakeholders, such as clinical and nonclinical staff and department/service leaders, participate in processes such as selection, testing, implementation, and evaluation of new and evolving health information technology systems.

Standard MOI.11

The hospital develops, maintains, and tests a program for response to planned and unplanned downtime of data systems.

Intent of MOI.11

Data systems are an important part of providing safe, high-quality patient care and downtime, whether planned or unplanned, can affect an entire system.

Guidance for MOI.11

Whether or not a hospital has implemented an electronic health record (EHR), a form of information technology exists in a majority of hospitals. Information technology can be found in digital imaging, laboratory testing and reporting of results, communication systems, pharmacy support systems, and the like.

Data system interruptions and failures, referred to as downtime, are unavoidable events. Planned downtime is scheduled for the purpose of conducting maintenance, repairs, upgrades, and other changes to the system. Unplanned downtime occurs as a result of power or equipment failures, heating/cooling system failures, natural disasters, human error, and interruptions to internet or intranet services, among other disruptions. Unplanned downtime can result in data system failures, such as loss of data, hardware failures, and data corruption. This can also result from cybersecurity threats or attacks. Hospitals may be in danger of permanently losing data if systems are not in place to copy and archive data.

Hospitals must prepare all departments and services with training specific to tactics and interventions for managing downtime in their particular area. When unplanned downtime occurs, staff need to be notified immediately upon discovery of the event.

The hospital must develop strategies and measures for continuing patient care during data system interruptions to maintain quality and safety. Following downtime, patient care and services provided during the period of downtime may need to be entered manually, through a document management/scanning system, or through transcriptions of hard copy to soft copy during periods of inactivity.

Recovery plans should be tested at least once a year. Simple backups should be tested at least once a quarter and whenever there is a major hardware or software change in the backup system. It is important to run a test after an upgrade to ensure the upgrade works properly with the rest of the systems.

The hospital plans for interruptions by:

- Training staff on alternative procedures
- Testing the hospital's emergency management program
- Conducting regularly scheduled data backups

- Testing data restoration procedures
- Addressing processes for continuity with electronic, paper-based, and/or knowledge-based information

Communication is essential to continuity of care during downtime. Notifying staff about planned downtime allows them to make necessary preparations to ensure that business continues in a safe and effective manner. Communication prior to planned downtime should include at least the following information:

- The information technology system or application that will be down and the department/service areas that will be affected
- The time that the downtime will begin and the expected length of time the system or application will be unavailable
- The reason for the downtime and what changes can be expected after the planned downtime is completed. **For example**, regular maintenance with no changes expected or an enhancement to the system.

Downtime recovery tactics must include disaster recovery and failover systems for backing up, recovering, and maintaining data systems. Recovery systems are typically located at remote locations to recover data that may have become corrupted or unintentionally deleted. These systems must be backed up periodically, usually every night. Failover systems minimize disruptions in patient care and loss of data and are usually on the premises and switched over within a few seconds or minutes of the primary system becoming unavailable due to planned or unplanned downtime. In hospitals that use a cloud-based system for data backup, the vendor must have adequate backup systems in place to minimize disruptions to care, prevent loss of data, and maintain data integrity.

Hospitals that plan for maintaining access to electronic information systems by using various backup and recovery processes are likely to experience seamless continuity of patient care and minimal data loss.

The manner in which information is communicated to staff will depend on the system that is down. **For example**, if the hospital's network goes down, communication to staff via telephone may be required. Multiple communication strategies should be developed in order to address the different systems that may be affected. In addition to internal communication strategies, it may be necessary to develop strategies for external communication. **For example**, if the hospital has an interfacing application with outside/contracted laboratory or radiology services and it becomes unavailable due to downtime, there needs to be a process for obtaining the results during downtime and a plan to have results reported back via the interface when the downtime is over.

One approach to managing downtime may include the practice of having a packet of hard-copy downtime forms or a downtime binder available to continue care if unplanned downtime exceeds a certain time threshold (typically greater than 30 minutes). Another approach may be to maintain a downtime computer that allows read-only access to patient data.

Organizations need to define what data may need to be reentered in a discreet format (**for example**, all medications prescribed during downtime, select orders, allergies, problem lists, and so on), what data may need to be scanned in, and what data may need to be transcribed from hard copy to soft copy. To ensure confidentiality and security of information, the organization should have a documented process for the management of any paper documentation used during downtime.

Many tools are available for backing up data. The optimal backup solutions for each hospital depend on many factors, including the amount of data requiring backup, the speed at which data can be backed up and recovered, the location of recovery systems, costs, and other factors.

Measurable Elements of MOI.11

- 1. The hospital maintains, and tests at least annually, a program for response to planned and unplanned downtime of data systems.
- 2. The hospital identifies the probable impact that planned and unplanned downtime of data systems will have on all aspects of care and services.
- 3. The program includes continuity strategies for the provision of ongoing safe, high-quality patient care and services, including services provided by outside vendors, during planned and unplanned downtime of data systems.
- 4. The program identifies internal and, when applicable, external communication strategies for planned and unplanned downtime.

CONFIDENTIAL PROPOSED REQUIREMENTS FOR FIELD REVIEW PURPOSE ONLY
DO NOT COPY – DO NOT DISTRIBUTE

- ❑ 5. The hospital implements downtime recovery tactics and ongoing data backup processes to recover and maintain data and ensure data integrity and maintain confidentiality and security of patient information.
 - ❑ 6. Staff are trained in the strategies and tactics used for planned and unplanned downtime of data systems.
-

Standard MOI.12

The hospital develops and maintains processes and procedures for cybersecurity and cyber risk management.

Intent of MOI.12

Cybersecurity in healthcare carries more risk due to the type and widespread use of information and can be detrimental to patient safety and hospital operations if not properly managed.

Guidance for MOI.12

Cyber-attacks have the potential to interrupt and delay a variety of services throughout a hospital system including ambulance transport, surgeries, medication delivery, and system operations (HVAC) to name a few. Information technology, whether in the form of the electronic health record (EHR) or that used throughout the hospital system is susceptible to cyber-attacks. As technology advances within the system, cybersecurity advancements need to be made as well to ensure patient safety and prevent operational delays. Areas that are vulnerable to cyber-attacks include, but are not limited to:

- EHR
- E-prescribing software
- Remote patient monitoring
- Laboratory information systems
- Medical billing software
- Scheduling software
- Communication systems

Measures and procedures for cybersecurity are necessary to protect valuable patient information during attacks. Downtime related to cyber events requires a differentiated plan from the standard planned or unplanned downtime for organizations that use an electronic health record and communication system. In the event of a cyber event, there must be a process to report details to the IT department, hospital leadership, and a cyber team if applicable.

Most departments in the hospital handle information that is highly sensitive and valuable to cyber hackers. Staff including providers of care, billing agents, administrative staff, and scheduling agents manage this information daily and require specialized training to understand safe practices and consequences of a cyber-attack or breach. Initial and ongoing training should be conducted and documented for completion.

In many healthcare organizations, resources allocated to the IT department may be limited due to a number of constraints. Leadership must consider all the medical devices that are interconnected throughout the system, the thousands of people using those devices, and inconsistent business/user processes.

In the event downtime occurs because of a cyber-attack, there must be downtime recovery procedures for backing up, maintaining, and potentially recovering system data. There is no single correct way to manage a cyber-attack, but having plans in place beforehand can reduce the impact. Both the US National Institute of Standards and Technology (NIST) and European Union Agency for Network and Information Security (ENISA) have frameworks for establishing a risk-based approach.

A strong posture for security includes:

- Having a quality, stable application base and infrastructure (**for example**, hardware, software applications, operating systems, networking tools, and telecommunication tools)
- Having IT infrastructure with configuration management, change management, logging, and monitoring

CONFIDENTIAL PROPOSED REQUIREMENTS FOR FIELD REVIEW PURPOSE ONLY

DO NOT COPY – DO NOT DISTRIBUTE

- Having a proactive stance and security measures in place (**for example**, resources and budgeting)
- Having training and awareness for all employees who interact in any way with hospital technology

Tactics for reducing exposure to a cyber-attack include, but are not limited to:

- Filtering email and checking suspicious content
- Updating security configurations on devices, servers, and systems
- Installing antivirus software
- Running penetration tests
- Limiting control of physical access
- Maintaining regularly scheduled backups, which are stored in a physical, offline place

Provisions should be made for communicating a security breach internally and notifying any affected party externally. **For example**, the General Data Protection Regulation (GDPR) implemented regulations for breach notification and penalties when not adhered to.

Measurable Elements of MOI.12

- 1. The hospital establishes and maintains an incident response program that includes
 - a) Identifying the probable impact a cyber-attack on data systems will have on all aspects of care and operations
 - b) Identifying strategies for the provision of ongoing safe and quality care and services
- 2. The program identifies internal and external communication strategies for those affected by cyber-attacks or events.
- 3. The hospital identifies the frequency of periodic review and evaluation of the program
- 4. The hospital implements recovery tactics and ongoing data backup processes to recover and maintain data, ensuring data integrity, confidentiality, and security.

References

Information Management

- Abouelmehdi K, Beni-Hessane A, Khaloufi H. Big healthcare data: Preserving security and privacy. *Big Data*. Epub 2018 Jan 9. <https://doi.org/10.1186/s40537-017-0110-7>.
- AHIMA. “Migrating from Paper to EHRs in Physician Practices - Retired” <https://library.ahima.org/doc?oid=103171>
- Arain MA, Tarraf R, Ahmad A. Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization. *J Multidiscip Healthc*. 2019 Jan 9;12:73–81.
- Bleiberg H, et al. A need to simplify informed consent documents in cancer clinical trials. A position paper of the ARCAD Group. *Ann Oncol*. 2017 May 1;28(5):922–930.
- Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*. 2018 Jul;113:48-52. doi: 10.1016/j.maturitas.2018.04.008. Epub 2018 Apr 22. PMID: 29903648.
- Fernandez-Aleman JL, et al. Technical solutions for mitigating security threats caused by health professionals in clinical settings. *Conf Proc IEEE Eng Med Biol Soc*. 2015 Aug;2015:1389–1392.
- Hepp SL, et al. Evaluation of the awareness and effectiveness of IT security programs in a large publicly funded health care system. *Health Inf Manag*. 2018 Sep;47(3):116–124.
- Institute for Safe Medication Practices. *ISMP’s List of Error-Prone Abbreviations, Symbols, and Dose Designations*. Oct 2, 2017. Accessed Jan 6, 2020. <https://www.ismp.org/tools/errorproneabbreviations.pdf>.
- Jayabalan M, O’Daniel T. Access control and privilege management in electronic health record: A systematic literature review. *J Med Syst*. 2016 Dec;40(12):261.
- Kruse CS, et al. Security techniques for the electronic health records. *J Med Syst*. 2017 Aug;41(8):127.
- Moon S, McInnes B, Melton GB. Challenges and practical approaches with word sense disambiguation of acronyms and abbreviations in the clinical domain. *Health Inform Res*. 2015 Jan;21(1):35–42.
- Rezaeibagha F, Win KT, Susilo W. A systematic literature review on security and privacy of electronic health record systems: Technical perspectives. *Health Inf Manag*. 2015;44(3):23–38.

Sharp K, et al. Conversion of provider EMR training from instructor-led training to eLearning at an academic medical center. *Appl Clin Inform.* 2017 Jul 26;8(3):754–762.

Sher ML, et al. How can hospitals better protect the privacy of electronic medical records? Perspectives from staff members of health information management departments. *Health Inf Manag.* 2017 May;46(2):87–95.

Zakaria H, et al. A systematic literature review of security perimeter in hospital facility. *Open International Journal of Informatics.* 2018;6(4):104–129. Accessed Jan 5, 2020. <http://apps.razak.utm.my/ojs/index.php/oiji/article/view/68/49>.

Management and Implementation of Documents

Salomi MJA, Maciel RF. Document management and process automation in a paperless healthcare institution. *Technol Invest.* 2017 Aug;8(3):167–178. <https://doi.org/10.4236/ti.2017.83015>.

Patient Medical Record

ECRI Institute, Partnership for Health IT Patient Safety. *Health IT Safe Practices: Toolkit for the Safe Use of Copy and Paste.* Feb 2016. Accessed Jan 5, 2020. https://www.ecri.org/Resources/HIT/CP_Toolkit/Toolkit_CopyPaste_final.pdf.

The Joint Commission. Preventing copy-and-paste errors in EHRs. *Quick Safety*, Issue 10. Feb 2015. Accessed Jan 6, 2020. https://jointcommission.org/assets/1/23/Quick_Safety_Issue_10.pdf.

Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal.* 2021 Jul; 22 (2): 177-183.

Monte AA, et al. Accuracy of electronic medical record medication reconciliation in emergency department patients. *J Emerg Med.* 2015 Jul;49(1):1:78–84. <https://doi.org/10.1016/j.jemermed.2014.12.052>.

Ryan TP, et al. Medication adherence, medical record accuracy, and medication exposure in real-world patients using comprehensive medication monitoring. *PLoS One.* 2017 Sep 28;12(9):e0185471. <https://doi.org/10.1371/journal.pone.0185471>.

Sprey E. The dangers of copy and paste in the EHR. *Physicians Practice.* Epub 2016 Oct 21. Accessed Jan 6, 2020. <http://www.physicianspractice.com/ehr/dangers-copy-and-paste-ehr>.

Telenti A, Steinhubl SR, Topol EJ. Rethinking the medical record. *Lancet.* 2018 Mar 17;391(10125):1013. [https://doi.org/10.1016/S0140-6736\(18\)30538-5](https://doi.org/10.1016/S0140-6736(18)30538-5).

Tsou AY, et al. Safe practices for copy and paste in the EHR. Systematic review, recommendations, and novel model for health IT collaboration. *Appl Clin Inform.* 2017 Jan 11;8(1):12–34.

Information Technology in Health Care

Argaw, S, et al. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making.* 2020; 20:146

Arunachalam S, Page T, Thorsteinsson G. Healthcare data warehousing. *i-Manager's Journal on Computer Science.* 2017 Dec–Feb;4(4):1–13.

Balch Samora J, et al. Mobile messaging communication in healthcare: Rules, regulations, penalties, and safety of provider use. *JBJS Rev.* 2018 Mar;6(3):e4. <https://doi.org/10.2106/JBJS.RVW.17.00070>.

Bhavnani SP, Narula J, Sengupta PP. Mobile technology and the digitization of healthcare. *Eur Heart J.* 2016 May 7;37(18):1428–1438. <https://doi.org/10.1093/eurhearti/ehv770>

ECRI Institute, Partnership for Health IT Patient Safety. *Safe Practice Recommendations for Developing Implementing, and Integrating a Health IT Safety Program.* Mar 2018. Accessed Jan 6, 2020. https://www.ecri.org/Resources/HIT/Health_IT_Safety/HIT_Toolkit_2018.pdf.

Goldfarb J, et al. Smartphones and patient care: Exploring the use of text-based messaging for patient related communication. *Surg Innov.* 2016 Jun;23(3):305–308.

Grossman LV, et al. Implementation of acute care patient portals: Recommendations on utility and use from six early adopters. *J Am Med Inform Assoc.* 2018 Apr 1;25(4):370–379.

The Joint Commission. Update: Texting orders. *Jt Comm Perspect.* 2016 May;36(5):15.

Khanna RR, Wachter RM, Blum M. Reimagining electronic clinical communication in the post-pager smartphone era. *JAMA.* 2016 Jan 5;315(1):21–22.

Newhouse N, et al. Patient use of email for health care communication purposes across 14 European countries: An analysis of users according to demographic and health-related factors. *J Med Internet Res.* 2015 Mar 6;17(3):e58.

Nguyen C, et al. The use of technology for urgent clinician to clinician communications: A systematic review of the literature. *Int J Med Inform.* 2015 Feb;84(2):101–110.

Oral B, et al. Downtime procedures for the 21st century: Using a fully integrated health record for uninterrupted electronic reporting of laboratory results during laboratory information system downtimes. *Am J Clin Pathol.* 2015 Jan;143(1):100–104.

Poterack KA, Gottlieb O, Rothman BS. Paper charting anesthetics: Forgotten but not gone . . . especially during an EHR downtime. *ASA Monitor.* 2017 Apr;81:30–32.

Serrano KJ, et al. Willingness to exchange health information via mobile devices: Findings from a population-based survey. *Ann Fam Med.* 2016 Jan–Feb;14(1):34–40. <https://doi.org/10.1370/afm.1888>.

CONFIDENTIAL PROPOSED REQUIREMENTS FOR FIELD REVIEW PURPOSE ONLY
DO NOT COPY – DO NOT DISTRIBUTE

Healthcare Technology (HCT)

Overview

The healthcare industry is facing a fast-moving digital revolution. Organizations are adopting new methods of technology to streamline processes and procedures and reduce costs. From electronic health records (EHR) to telehealth capabilities, artificial intelligence, and medical equipment advancements, technological innovations have enhanced clinical outcomes, improved patient care, and transformed the possibilities for care delivery.

As the demand for specialized healthcare services continues to increase, technology will continue to play a critical and necessary role in the comprehensive care process. Management of technology and medical equipment requires a high level of communication and collaboration to maintain an integrated system of care, services, and providers that make up the continuum of care. Establishing processes and procedures for efficient integration and oversight is paramount for success.

Standards

The following is a list of all standards for this function. They are presented here for your convenience without their intent statements or measurable elements. For more information about these standards, please see the next section in this chapter, Standards, Intents, Guidance, and Measurable Elements.

Information Technology in Health Care

- HCT.1 Hospital leadership identifies a qualified individual to oversee the hospital's health information technology and processes.
- HCT.2 When mobile devices are used for texting, e-mailing, or other communications of patient data and information, the hospital implements processes to ensure quality of patient care and maintains security and confidentiality of patient information.
- HCT.3 For organizations providing telehealth services, the hospital implements guidelines for the protection of patient data and information that is in compliance with local laws and regulations.
- HCT.4 For hospitals using clinical decision support tools, there are methods for oversight and processes for improvement implemented by a qualified individual.

Management of Lasers

- HCT.5 The hospital establishes and implements a program for the safe use of lasers and other optical radiation devices used for performing procedures and treatments.

Medical Equipment

- HCT.6 The hospital develops and implements a program for the management of medical equipment throughout the organization.
- HCT.7 The hospital has a process for monitoring and acting on medical equipment hazard notices, recalls, reportable incidents, problems, and failures.

Standards, Intents, Guidance, and Measurable Elements

**CONFIDENTIAL PROPOSED REQUIREMENTS FOR FIELD REVIEW PURPOSE ONLY
DO NOT COPY – DO NOT DISTRIBUTE**

Information Technology in Health Care

Standard HCT.1

Hospital leadership identifies a qualified individual to oversee the hospital's health information technology and processes.

Intent of HCT.1

Technology systems can be complex and require oversight for successful implementation and coordination with existing processes.

Guidance for HCT.1

Investment in information technology is an important resource for hospital systems. Technology systems and processes can significantly improve efficiency, patient safety, dissemination of data, and error reduction.

Health information technology includes:

- Electronic health records for documentation and information sharing
- Patient portals
- Systems for storing, managing, and securing data
- Platforms for communication among health care practitioners for care coordination
- Interfaces with other systems to facilitate patient care and treatment
- Electronic prescribing tools
- Telehealth technology- and applications
- Medical billing software

Without proper evaluation and testing, health information technology can pose increased risks to patients. Successful implementation and integration of health information technology systems requires resources and direction from hospital leaders. The leadership team appoints a qualified individual to oversee technological systems and processes. A qualified individual has education, training, and/or experience relevant to the role and responsibilities.

The hospital's information technology systems must be managed effectively and in a comprehensive and coordinated manner. The individual who oversees the health information technology systems is responsible for at least the following:

- Recommending space, equipment, technology, and other resources to hospital leaders to support information technology systems in the hospital
- Selecting and testing new technologies/systems
- Conducting risk assessments to assess security risks, prioritize risks, and identify improvements
- Ensuring staff are educated and trained on technology security, applicable policies, and procedures
- Implementing metrics to assess how technology systems are functioning and impacting hospital operations

When technology systems are implemented, it is important for the hospital to establish a process to evaluate their usability and effectiveness. Evaluation includes

- Whether or not the technology is being used as designed and intended
- How well the technology integrates with existing technologies
- What effects technology has on improving patient safety, reducing errors, and enhancing performance
- What effect technology has on staff (**for example**, increasing efficiency, increasing or reducing stress and burnout)

CONFIDENTIAL PROPOSED REQUIREMENTS FOR FIELD REVIEW PURPOSE ONLY
DO NOT COPY – DO NOT DISTRIBUTE

Depending on the size and scope of the organization, there may be several individuals who support the point person to manage aspects of the program. This individual may also have responsibilities with the health information systems.

All or part of integrating new and existing health information technology may be done through contracted services. Oversight of the contract is provided by the individual who oversees health information technology.

Measurable Elements of HCT.1

- 1. Hospital leadership provides support and resources for technology services in the hospital.
 - 2. Hospital leadership identifies a qualified individual to oversee technological systems and processes.
 - 3. Hospital leaders and a qualified individual(s) participate in processes such as selection, testing, implementation, and evaluation of new and evolving health information technology systems. This includes:
 - a) Recommendations for space, equipment, and resources
 - b) Selection and testing of new technology or systems
 - c) Oversight of risk assessments to assess security risks, prioritize risks, and identify improvements
 - d) Education of staff on technology security, applicable policies, and procedures
 - e) Implementation of metrics to assess how technology systems are functioning and impacting hospital operations
 - 4. New and evolving health information technology systems are monitored and evaluated for usability, effectiveness, intended use by staff, and patient safety, and improvements are identified and implemented based on results.
-

Standard HCT.2

When mobile devices are used for texting, e-mailing, or other communications (**for example**, WhatsApp) of patient data and information, the hospital implements processes to ensure quality of patient care and maintains security and confidentiality of patient information. The hospital only utilizes these communication platforms when allowed by the local regulations and policies.

Intent of HCT.2

Time-sensitive data sent via email may not be viewed by the physician in a timely manner and delay immediate actions that may be needed. The information may be secured on the physician or hospital side, but the patient may not have the same securities in place.

Guidance for HCT.2

As technology has evolved, many health care practitioners have begun to use mobile devices to

- Communicate patient data and information through text messages and emails (critical results, referrals, and notes)
- Exchange communications with other practitioners
- Receive text messages or emails from patients

Hospitals may provide mobile devices to their health care practitioners or may allow practitioners to use their personal devices. When mobile devices are used, the hospital needs to ensure that patient data and information are kept secure and confidential, in accordance with laws and regulations, and hospital policy. When the mobile devices are provided to staff by the hospital, there are procedures to retrieve the devices when staff are no longer employed by or associated with the hospital.

When the hospital allows confidential and private patient information to be transmitted through text messaging (**for example**, patient identification, diagnoses, history, test results, and other confidential information), the hospital ensures that a secure messaging platform is implemented and includes the following:

- Secure, encrypted sign-on processes for authentication of users (password protected, unique to each user, and end-to-end encrypted for all contents)
- Processes for ensuring that only authorized individuals are in the platform directory for receiving messages
- Delivery and read receipts for messages
- Date and time stamp for messages
- Processes for protecting and securing patient information against unauthorized access and use

The hospital establishes processes for ensuring that email or text messages with patient information are documented in the medical record when the content relates to the care of the patient. **For example**, text messages exchanged among health care practitioners that contain information used to make decisions about a patient's care need to be documented in that patient's medical record.

Patient portals also allow communication between practitioners and patients and provide a range of services that can be performed online or through an app on a mobile device, such as

- Completing registration forms
- Requesting prescription refills
- Accessing test results
- Scheduling nonurgent appointments
- Sending/receiving messages with the physician
- Downloading educational materials
- Making electronic payments.

Hospitals that implement patient portals ensure confidentiality and security of the patient information stored and exchanged through the portal. The implementation and use of patient portals require encryption of patient data/information, secure, sign-on process with password requirements for users, audit trails that log and record key activities, and consent from patients to participate in the patient portal.

Data confidentiality can be achieved in several ways including

- Implementation of access controls with authentication
- Establishing a secure password policy as defined by the organization (**for example**, minimum number of characters, use of special characters, combination of letters and numbers, use of uppercase and lowercase letters, password renewal schedule throughout the year)
- Implementation of remote access to disable or remove patient data from mobile devices in the event they are lost or stolen
- Enhanced security controls
- Limiting email use to areas where risk of breach of confidentiality or delay in response is lower

The hospital, where applicable, implements a process to monitor the quality of communications conducted through text, e-mail, and patient portals, and makes improvements where needed. The hospital ensures that patients have adequate understanding of data and information received through text, e-mail, and patient portals, and encourages patients to contact their health care provider for questions. The hospital collects data to monitor the process for clarifying questions that arise from messages received via text, e-mail, and patient portals. **For example**, the hospital may collect data on how often staff need to clarify patient information that has been texted and the process for obtaining clarification.

Measurable Elements of HCT.2

- 1. When patient data and information is transmitted through text messaging, the hospital ensures that the process is through a secure messaging platform and complies with the following

**CONFIDENTIAL PROPOSED REQUIREMENTS FOR FIELD REVIEW PURPOSE ONLY
DO NOT COPY – DO NOT DISTRIBUTE**

- a) Secure, encrypted sign-on processes for authentication of users (password protected and unique to each user)
 - b) Processes for ensuring that only authorized individuals are in the platform directory for receiving messages
 - c) Delivery and read receipts for messages
 - d) Date and time stamp for messages
 - e) Processes for protecting and securing patient information against unauthorized access and use
- 2. When mobile devices are used for communicating patient data and information, the hospital implements guidelines and processes to protect and secure patient information.
 - 3. The hospital establishes processes to ensure that text messages and e-mails on mobile devices that have data and information relating to a patient's care are documented in the patient's medical record.
 - 4. When the hospital implements a patient portal or communicates with patients via text messages or e-mails, the hospital
 - a) Educates the patient on the patient portal and confirms readiness for use
 - b) Obtains consent from patients to participate in the portal and/or receive text messages or e-mails
 - 5. When the hospital allows patient information to be communicated via text messages, e-mail, and patient portals, the hospital has a process to ensure that questions that arise about the information exchanged are addressed in a timely manner and monitors for improvements needed to the communication processes.

Standard HCT.3

For organizations providing telehealth services, the hospital implements guidelines for the protection of patient data and information.

Intent of HCT.3

Established guidelines for telehealth services provide a framework for standardization, safety, securing, and quality of care.

Guidance for HCT.3

Telehealth requires a more comprehensive and integrated approach for delivery of patient care. A high degree of collaboration and communication among health care providers is mandatory for successful implementation.

A hospital providing telehealth services should establish a framework for delivering patient services in a consistent manner, regardless of the physical location of the patient or provider. Having a standardized process for providing services results in best practice, efficient use of resources, and improved patient outcomes. Providers operating within an integrated system will ensure a “seamless delivery” of care and services. The processes in place shall ensure integration measures to prevent fragmentation of data.

The hospital implements guidelines to ensure patient data and information remains confidential and that telehealth services are secure from data breaches and other cybersecurity threats. This begins with an effective employee training program.

Data breaches can result in harm to patients and potential fines to the organization. Hospitals using telehealth platforms should implement processes to ensure data is correct and remains confidential to prevent inappropriate delivery of care. Methods that may be used include

- Multifactor authentication
- Decentralized storage of data
- Encrypted data
- Use of secured networks or virtual private networks (VPN)
- Employee training programs must include cybersecurity awareness with specific topics that ensure security of confidential information.

Measurable Elements of HCT.3

- 1. The hospital implements guidelines and processes to secure patient information when telehealth services are utilized.
- 2. The hospital establishes processes to ensure that patient information remains confidential when telehealth services are utilized.
- 3. The hospital establishes processes to ensure the integration of information when multiple touchpoints and platforms within the system are used.
- 4. All staff involved in providing telehealth services receive cyber safety training and continuing education and the training and ongoing education are documented. Training includes:
 - a) Device security
 - b) Access privileges
 - c) Password protection
 - d) Social engineering and phishing
 - e) Cybersecurity threats

**CONFIDENTIAL PROPOSED REQUIREMENTS FOR FIELD REVIEW PURPOSE ONLY
DO NOT COPY – DO NOT DISTRIBUTE**

Standard HCT.4

For hospitals using clinical decision support tools, there are methods for selection and approval prior to implementation, oversight, and mechanisms for ongoing evaluation implemented by a qualified individual.

Intent of HCT.4

Artificial intelligence technology is rapidly progressing within the healthcare setting and requires guidelines to ensure biases are avoided, ethical standards are maintained, information is stored privately and securely, and the tools are performing as intended to meet expectations of the end users.

Guidance for HCT.4

Artificial intelligence (AI) advancements are providing opportunity for healthcare organizations to improve outcomes, reduce organizational costs, and impact public health. AI-based decision support tools are being implemented across multiple settings and specialties within healthcare settings to transform decision making processes. These tools are used to improve quality of care, increase efficiency in the delivery of care, and enhance decision making by analyzing patient data and generating predictions based on that data. Machine learning and algorithms analyze data, learn from patterns or trends, and offer insight to healthcare providers across the continuum.

A qualified individual, identified by relevant training and background, as well as the leadership team and key stakeholders should be involved in the selection process and ongoing oversight of AI tools. Hospitals using AI technology should have methods in place to evaluate the decision-making support tools to ensure they meet expectations of the organization and patient population. Ongoing monitoring is necessary for usability, intended use, up to date capabilities, data safety, data quality, system risks, and any ethical concerns. There should also be consideration that a human practitioner is involved in final decision making when it involves patient care. Practitioners should still physically examine patients, review any documentation prompts, and be held responsible for the care of the patient. The hospital should establish a process for reporting any adverse outcomes to the leadership team and key stakeholders.

Education and training of all pertinent staff members who interact with the AI decision support tools is required to ensure effective and safe integration into practice and care delivery. Having established users onsite to troubleshoot or provide training sessions can be beneficial to the organization.

AI clinical decision support tools include diagnostic decision support tools, treatment decision support tools, predictive analytics tools, and population health management tools. **Examples** of commonly used types of clinical decision support tools used in the hospital setting include, but are not limited to:

- Sepsis triggers
- Wound management
- Medication reconciliation
- Medication dosing
- Diagnostic code selection
- Aide in rapid response procedures
- Creation of treatment guidelines for urgent conditions
- Interpretation of lab and testing results

Factors to consider when assessing the AI technology and algorithms are

- Is it meaningful or useful to the setting?
- Is it providing up to date data?

**CONFIDENTIAL PROPOSED REQUIREMENTS FOR FIELD REVIEW PURPOSE ONLY
DO NOT COPY – DO NOT DISTRIBUTE**

- Does it meet clinical workflow expectations?
- What is the impact on clinical decision making?
- What is the confidence level of the output data?

Monitoring effective use of AI technology for clinical decision making includes

- Reviewing usage logs including common uses, areas for improvement, user satisfaction
 - Identifying discrepancies in diagnoses, treatment recommendations, or medications
 - Analyzing feedback from providers
 - Evaluating patient outcomes
 - Performing updates to the tool or the system
-

Measurable Elements of HCT.4

- 1. The hospital identifies qualified individuals to select the relevant AI tools for their respective areas of expertise (**for example**, pharmacy, wound care, surgery, etc)
 - 2. The hospital establishes guidelines and processes for oversight of the effectiveness of AI tools used by the organization. This includes
 - a) Approval and implementation processes
 - b) Human practitioner involvement in final decision making of patient care
 - c) Security and privacy of patient data
 - d) Identification of system discrepancies
 - e) Analysis from providers and relevant third-party sources
 - f) Updates to software/technology as deemed appropriate
 - 3. The hospital tracks usage and trends on an ongoing basis and reports outcomes to the relevant parties (**for example**, key stakeholders, leadership team, third party sources, etc)
-

Management of Lasers

Standard HCT.5

The hospital establishes and implements a program for the safe use of lasers and other optical radiation devices used for performing procedures and treatments.

Intent of HCT.5

Nearly all lasers and optical radiation devices that are used in the clinical setting pose potential hazards for patients and staff if safety procedures and guidelines are not established and followed.

Guidance for HCT.5

Lasers are a source of optical radiation, which includes ultraviolet radiation, high-intensity visible light, and infrared radiation. The narrow beam of high-intensity light from a laser can be targeted and focused for precise surgical

**CONFIDENTIAL PROPOSED REQUIREMENTS FOR FIELD REVIEW PURPOSE ONLY
DO NOT COPY – DO NOT DISTRIBUTE**

procedures. As technology evolves, the use of lasers is becoming more common with surgical procedures and their clinical use is broadening.

Laser surgeries are generally minimally invasive with less blood loss than conventional surgery, and patients typically experience shorter recovery times. Lasers are also used in noninvasive procedures providing safer alternatives for treating conditions without surgical intervention.

Lasers and optical radiation devices can generate intense concentrations of heat, light, and reflected light. When the skin and eyes are exposed to the heat and light without adequate protection, skin burns and eye injuries, such as retinal burns, cataracts, and macular degeneration, may result. Injuries can come from direct contact with the light or with the reflected light from the laser.

Laser plumes are another potential hazard. These are the vapors, smoke, and particles produced during some surgical procedures. Laser plumes introduce a potential respiratory hazard for patients and staff, as they may contain irritants, toxins, tissue, bacteria, viruses, blood fragments, and other particles, depending on the type of procedure.

To prevent these hazards and address safety risks to patients and staff, the hospital establishes and implements a program for the safe use of lasers and other optical radiation devices using industry standards and professional guidelines. The program complies with laws and regulations and includes the following:

- A qualified individual who has oversight and supervision of the laser and optical radiation safety program
- Training in safety practices and procedures for all staff who are involved in the use of lasers and optical radiation devices
- Ongoing education and training are provided for new procedures, practices, devices, and equipment
- Documentation of training and ongoing education
- Administrative and engineering controls to promote safety and prevent injury
- Availability of personal protective equipment for staff and patients appropriate to the type of laser or optical radiation device being used or type of procedure performed in the hospital (**for example**, goggles, corneal shields, masks, gloves, and/or gowns as applicable)
- A maintenance program for lasers and optical radiation devices and a process for routine performance checks such as calibration and alignment
- Coordination with the facility management and infection prevention and control programs; all facility safety events and infection control events need to be reported
- Detecting and reporting adverse health effects and identifying and implementing improvements to prevent recurrence

Laser surgery interventions include:

- LASIK and cataract surgery
- Removal of skin lesions
- Treatment of varicose veins
- Dentistry procedures to remove tooth decay or recontour soft tissue

Noninvasive, optical radiation treatments can include:

- Intense pulsed light therapy to treat skin conditions
- Ultraviolet radiation to treat psoriasis
- Lasers to whiten teeth
- High-intensity visible light for dental procedures
- Light therapy for treatment of pain and inflammation
- Infrared radiation to treat strained muscles and soft tissue

Adverse events resulting from the use of lasers and other optical radiation devices are reported, and action plans to prevent recurrence are implemented and monitored. Controls used to promote safety and prevent injury are implemented. **Examples** include

- Criteria and processes for authorizing staff who enter and/or work in the areas (hazard zones) where lasers and other optical radiation is used
- The hospital identifies any additional staff who may require access to hazard zones
- Warning signs placed outside procedure areas to alert staff, patients, families, and visitors when a treatment or procedure is being performed
- Appropriate ventilation to help manage smoke plumes
- Use of nonreflective instruments to prevent exposures to reflective light
- Use of drapes and other barriers to prevent staff, patients, families, and visitors from inadvertently being exposed to direct or reflected light

Measurable Elements of HCT.5

- 1. The hospital's program for the safe use of lasers and optical radiation devices is
 - a) Based on industry standards and professional guidelines and complies with applicable laws and regulations
 - b) Part of the hospital's facility management and safety structure and provides reports at least annually and when any safety events occur
- 2. A qualified individual with the appropriate training and experience has oversight and supervision of the laser and optical radiation safety program.
- 3. All staff involved in the use of lasers and optical radiation devices receive safety training and continuing education; the training and ongoing education are documented.
- 4. The hospital establishes and implements administrative and engineering controls for the laser and optical radiation safety program to promote safety and prevent injury for patients and staff.
- 5. Personal protective equipment appropriate to the type of lasers and optical radiation devices and type of procedures is available for staff and patients, and staff use it correctly and ensure that patients are protected during procedures.
- 6. The hospital has processes for inspection, testing, and maintenance of lasers and optical radiation devices, including routine calibration and alignment checks of lasers, and these activities are performed by qualified and trained individuals.

Medical Equipment

Standard HCT.6

The hospital develops and implements a program for the management of medical equipment throughout the organization.

Intent of HCT.6

Management of medical equipment is performed to ensure that all equipment is functioning properly and available for use.

Guidance for HCT.6

The medical equipment management program includes

- An inventory of all medical equipment

**CONFIDENTIAL PROPOSED REQUIREMENTS FOR FIELD REVIEW PURPOSE ONLY
DO NOT COPY – DO NOT DISTRIBUTE**

- Regular inspections
- Testing according to use and manufacturer requirements
- Documentation of results
- Performance of preventative maintenance, significant repairs, and disposal when necessary
- Documentation of all repair work completed

As part of the medical equipment program, the hospital conducts and documents a risk assessment, at least annually, to identify areas in which medical equipment risks exist.

Medical equipment management is performed by a qualified individual(s) based on background experience, education, and training. Medical equipment is utilized by departments throughout the organization (**for example**, facilities team, bioengineering team, and environmental services) and should have unified management processes to maintain an integrated system. Testing and inspection are performed when equipment is new and then on an ongoing basis according to age, use, and manufacturers' instructions. Inspections, testing results, any maintenance, and repairs are documented to ensure continuity of processes and guide capital planning for replacements, upgrades, and other changes.

Measurable Elements of HCT.6

- 1. The hospital develops and implements a written program for the management of medical equipment that is hospital owned and non-hospital owned (leased, rented, patient owned)
- 2. **The equipment program includes:**
 - a) **An inventory of all medical equipment**
 - b) **Regular inspections when equipment is new and as requested by manufacturer guidelines**
 - c) **Testing according to use and manufacturers' requirements**
 - d) **Documentation of results**
 - e) **Performance of preventative maintenance and calibration as applicable**
- 3. A medical equipment risk assessment is conducted and documented annually throughout the hospital, and medical equipment risks are identified and prioritized from the risk assessment.
- 4. The hospital identifies goals, implements improvements, and monitors data to ensure that medical equipment risks are reduced or eliminated.

Standard HCT.7

The hospital has a process for monitoring and acting on medical equipment hazard notices, recalls, reportable incidents, problems, failures, repairs, or refurbishment, and for validating effectiveness of those actions.

Intent of HCT.7

Medical equipment malfunctions pose risks to patients, providers, and other staff members and having processes in place ensures awareness of issues and allows for action to prevent harm.

Guidance for HCT.7

The hospital has a system in place for monitoring and acting on medical equipment hazard notices, recalls, reportable incidents, problems, and failures sent by the manufacturer, supplier, or regulatory agency. Some countries require reporting of any medical equipment that has been involved in a death, serious injury, or illness. Hospitals must identify and comply with the laws and regulations pertaining to the reporting of medical equipment incidents. The hospital conducts a root cause analysis in response to any sentinel events.

**CONFIDENTIAL PROPOSED REQUIREMENTS FOR FIELD REVIEW PURPOSE ONLY
DO NOT COPY – DO NOT DISTRIBUTE**

Measurable Elements of HCT.7

- 1. The hospital has a process for monitoring and acting on medical equipment and implantable device hazard notices, recalls, reportable incidents, problems, and failures.
- 2. The hospital reports any deaths, serious injuries, or illness that are a result of medical equipment through the hospital's incident and adverse event reporting process.
- 3. The medical equipment management program addresses the use of any medical equipment with a reported problem or failure, or that is the subject of a hazard notice or is under recall.

References

Information Technology in Health Care

- Arunachalam S, Page T, Thorsteinsson G. Healthcare data warehousing. *i-Manager's Journal on Computer Science*. 2017 Dec–Feb;4(4):1–13.
- Balch Samora J, et al. Mobile messaging communication in healthcare: Rules, regulations, penalties, and safety of provider use. *JBJS Rev*. 2018 Mar;6(3):e4. <https://doi.org/10.2106/JBJS.RVW.17.00070>.
- Bhavnani SP, Narula J, Sengupta PP. Mobile technology and the digitization of healthcare. *Eur Heart J*. 2016 May 7;37(18):1428–1438. <https://doi.org/10.1093/eurheartj/ehv770>
- ECRI Institute, Partnership for Health IT Patient Safety. *Safe Practice Recommendations for Developing Implementing, and Integrating a Health IT Safety Program*. Mar 2018. Accessed Jan 6, 2020. https://www.ecri.org/Resources/HIT/Health_IT_Safety/HIT_Toolkit_2018.pdf.
- Goldfarb J, et al. Smartphones and patient care: Exploring the use of text-based messaging for patient related communication. *Surg Innov*. 2016 Jun;23(3):305–308.
- Grossman LV, et al. Implementation of acute care patient portals: Recommendations on utility and use from six early adopters. *J Am Med Inform Assoc*. 2018 Apr 1;25(4):370–379.
- The Joint Commission. Update: Texting orders. *Jt Comm Perspect*. 2016 May;36(5):15.
- Khanna RR, Wachter RM, Blum M. Reimagining electronic clinical communication in the post-pager smartphone era. *JAMA*. 2016 Jan 5;315(1):21–22.
- Magrabi F, et al. Artificial Intelligence in Clinical Decision Support: Challenges for Evaluating AI and Practical Implications. *Yearb Med Inform*. 2019 Apr 25; 28(1): 128-134. <http://dx.doi.org/10.1055/s-0039-1677903>
- Newhouse N, et al. Patient use of email for health care communication purposes across 14 European countries: An analysis of users according to demographic and health-related factors. *J Med Internet Res*. 2015 Mar 6;17(3):e58.
- Nguyen C, et al. The use of technology for urgent clinician to clinician communications: A systematic review of the literature. *Int J Med Inform*. 2015 Feb;84(2):101–110.
- Serrano KJ, et al. Willingness to exchange health information via mobile devices: Findings from a population-based survey. *Ann Fam Med*. 2016 Jan–Feb;14(1):34–40. <https://doi.org/10.1370/afm.1888>.
- Sutton R, et al. An Overview of Clinical Decision Support Systems: Benefits, Risks, and Strategies for Success. *NPJ Digit Med*. 2020 Feb 6; 3: 17.

Management of Lasers

- Cressey BD, Keyes A, Alam M. Laser safety: Regulations, standards and practice guidelines. In Nouri K, editor: *Lasers in Dermatology and Medicine: Dermatologic Applications*, 2nd ed. Cham, Switzerland: Springer International, 2018, 37–47.
- Gupta P. Laser safety: Recommendations for lasers in healthcare. *Professional Safety*. 2018 Feb;63(2):59–60.
- He JX, et al. [Investigation of non-ionizing radiation hazards from physiotherapy equipment in 16 medical institutions]. *Zhonghua Lao Dong Wei Sheng Zhi Ye Bing Za Zhi*. 2013 Dec;31(12):900–901.
- Ilce A, et al. The examination of problems experienced by nurses and doctors associated with exposure to surgical smoke and the necessary precautions. *J Clin Nurs*. 2017 Jun;26(11–12):1555–1561.

Okoshi K, et al. Health risks associated with exposure to surgical smoke for surgeons and operation room personnel. *Surg Today*. 2015 Aug;45(8):957–965.

Parker PJ, Parker SPA. Laser safety. In Coluzzi DJ, Parker SPA, editors: *Lasers in Dentistry—Current Concepts*. Cham, Switzerland: Springer International, 2017, 87–106.

Pinto I, et al. Blue light and ultraviolet radiation exposure from infant phototherapy equipment. *J Occup Environ Hyg*. 2015;12(9):603–610.

Medical Equipment

Kutor Jk, Agede P, Ali RH. Maintenance practice, causes of failure and risk assessment of diagnostic medical equipment. *Journal of Biomedical Engineering and Medical Devices*. 2017;2(1):1000123. Accessed Jan 5, 2020. <https://www.longdom.org/open-access/maintenance-practice-causes-of-failure-and-risk-assessment-of-diagnostic-medical-equipment-2475-7586-1000123.pdf>.

Subhan, A. 2017 Joint Commission medical equipment standards. *J Clin Eng*. 2017 Apr–Jun;42(2):56–57.

World Health Organization. *Global Atlas of Medical Devices*. 2017. Accessed Jan 5, 2020. <http://apps.who.int/iris/bitstream/10665/255181/1/9789241512312-eng.pdf?ua=1>.

World Health Organization. *Medical Devices: Management and Use*. 2017. Accessed Jan 5, 2020. http://www.who.int/medical_devices/management_use/en/.