Measurable Elements of MOI.01.02

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 cyberattacks.
3. The hospital implements data security best practices to protect and secure data and information. (*See also* PCC.01.02, ME 1; HCT.01.01, MEs 1 and 2)
4. The hospital identifies goals, implements improvements to address data security risks, and monitors improvement data to ensure that risks are reduced or eliminated.
5. Ⓓ The hospital establishes a written policy with procedures to follow in the event a successful cyberattack occurs.

Standard MOI.01.03

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

Intent of MOI.01.03

The hospital determines the retention time of medical 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.

The retention process for medical records, data, and other information, including text messages and e-mails that contain information for medical records, is consistent with hospital policies and procedures for maintaining the confidentiality and security of such information. After the retention period, patient medical records, data, and other information are destroyed in a manner that does not compromise confidentiality and security.

Measurable Elements of MOI.01.03

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

Standard MOI.01.04

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.01.04

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.

This education and training enable these individuals to do the following:

- 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 medical 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 that 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. Examples include the following:

- "Tips and tricks"
- Quick reference guides
- Short educational modules
- Newsletters (posted or e-mailed)

Cybersecurity education and training topics can include the following:

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

Measurable Elements of MOI.01.04

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.
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, annual 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.

Standardized Use of Information

Standard MOI.02.00

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

Intent of MOI.02.00

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

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