Standard MOI.01.02

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 cyberattacks.

Intent of MOI.01.02

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

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

Vulnerabilities that pose a security risk include response to phishing e-mails, sending unencrypted e-mails, 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 medical 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 medical records in locations where they will be protected from heat, water, fire, pests, or infestation
- Storing active medical records in areas where only authorized health care practitioners have access
- Ensuring that server rooms and areas where physical medical records are stored are secured and accessible only by authorized individuals
- Ensuring that server rooms and areas where physical medical records are kept are at proper temperature and humidity levels to protect servers/records
- Ensuring that server rooms and areas where physical medical 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 that staff are trained, at least annually, in such topics as the following:

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

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.