- 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 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.01.00

1. The hospital selects processes to meet the information needs of the following:
   - Those who provide clinical services
   - The hospital's leaders and department/service leaders (*See also* GLD.03.02, MEs 1 and 2)
   - Individuals, services, and agencies outside the hospital (*See also* GLD.03.01, ME 2)
   - 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 of the hospital include the following:
   - The hospital's mission
   - Services provided
   - Resources
   - Access to affordable technology
   - Usability and interoperability assessments
   - Support for effective communication among caregivers

Standard MOI.01.01

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

Intent of MOI.01.01

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

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 medical record information.

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

- Patient medical 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 medical 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 medical 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.

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 the following:

- Who is authorized to have access to data and information, including patient medical 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 is 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 that user permissions are set appropriately according to current roles and 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 the following:

- Time frame 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.01.01

1. The hospital implements processes consistent with laws and regulations to ensure the confidentiality, security, and integrity of data and information. (*See also* PCC.01.02, ME 1)
2. Ⓓ The hospital identifies, in writing, those authorized to access data and information, including those authorized to make entries in the patient medical 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. (*See also* ACC.03.00, ME 2)
5. The hospital implements processes to ensure that only authorized individuals make entries in the patient medical 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.