Depending on the size and scope of the hospital, 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 or health information management.

Measurable Elements of HCT.01.00

1. Hospital leaders provide support and resources for technology services in the hospital.
2. Hospital leaders identify a qualified individual to oversee technological systems and processes. (*See also* GLD.06.00, ME 1)
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.
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.01.01

When patient data and information are sent electronically, via mobile devices or other forms of electronic communication, the hospital implements processes to ensure quality of patient care, compliance with local laws and regulations, and maintenance of security and confidentiality of patient information.

Intent of HCT.01.01

Time-sensitive data sent electronically 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.

As technology has evolved, many health care practitioners have begun to use electronic forms of communication to do the following:

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

These electronic forms of communication may include mobile devices, e-mail, and secure messaging platforms.

Hospitals may provide mobile or portable devices to their health care practitioners or may allow practitioners to use their personal devices. When mobile or portable 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 these 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, other confidential information), the hospital ensures that a formal, 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

If the content of the message cannot be guaranteed to be secure, confidential information should be excluded from the message. Sensitive patient information should not be sent through a less secure platform.

The hospital establishes processes for ensuring that e-mails 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 the following:

- 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, a secure, encrypted 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 the following:

- Implementation of access controls with authentication
- Establishing a secure password policy as defined by the hospital (for example, minimum number of characters, use of special characters, combination of letters and numbers, use of uppercase and lowercase letters, limited reuse of previous passwords, 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 e-mail use to areas where risk of breach of confidentiality or delay in response is lower

The hospital 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. Where applicable, the hospital abides by health information management rules or standards set by the country/region in which it operates.

Measurable Elements of HCT.01.01

1. When patient data and information are transmitted through mobile text messaging or electronic communication tools, the hospital ensures that the process is through a secure platform and complies with the following:
   - Secure, encrypted sign-on processes for authentication of users (password protected and unique to each user)
   - 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 (*See also* MOI.01.02, ME 3)
2. Ⓓ When mobile devices are used for communicating patient data and information, the hospital implements written guidelines and processes to protect and secure patient information. (*See also* MOI.01.02, ME 3)
3. The hospital establishes processes to ensure that information relating to a patient's care sent electronically (for example, through text messages or e-mails) is documented in the patient's medical record. (*See also* MOI.03.00, ME 4)
4. When the hospital implements a patient portal or communicates with patients via text messages or e-mails, the hospital does the following:
   - Educates the patient on the patient portal and confirms readiness for use. (*See also* PCC.04.00, ME 1)
   - 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-mails, 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.01.02

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

Intent of HCT.01.02

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

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. Patient data and information that would be entered into a medical record during an in-person visit must be incorporated into the medical record during a telehealth visit (for example, patient history, diagnosis, treatment, instructions).

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