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.

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

- Multifactor authentication
- Decentralized storage of data
- Encrypted data
- Use of secured networks or virtual private networks (VPNs)
- Access control monitoring

Employee training programs must include cybersecurity awareness with specific topics that ensure security of confidential information.

Measurable Elements of HCT.01.02

1. Ⓓ The hospital implements written guidelines and processes to secure patient information when telehealth services are used.
2. The hospital establishes processes to ensure that patient information remains confidential when telehealth services are used.
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 cybersecurity training and continuing education, and the training and ongoing education are documented. Training for staff accessing health information technology systems includes the following:
   - Device security
   - Access privileges
   - Password protection
   - Social engineering and phishing
   - Cybersecurity threats

Standard HCT.01.03

For hospitals using artificial intelligence clinical decision support tools, there are processes for selection, implementation, oversight, and improvement.

Intent of HCT.01.03

Artificial intelligence (AI) technology is rapidly progressing within the health care setting and requires guidelines to ensure that 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.

AI advancements are providing opportunity for hospitals to improve outcomes, reduce organizational costs, and impact public health. AI–based decision support tools are being implemented across multiple settings and specialties within health care 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 those data. Machine learning and algorithms analyze data, learn from patterns or trends, and offer insight to health care providers across the continuum.

The health care industry is one of a few whose clients turn to the Internet to search for their problems before consulting with a professional. Individuals research their symptoms online and have a tendency to diagnose themselves based on those search results. Countering the need for a growing demand of services, use of AI chatbots or technology of the like are on the rise. AI use in this manner can allow for these services to be provided to a wider population range, save time for providers, and increase data analysis capabilities. When incorporating chatbots, there is a concern for data to remain private, be safeguarded, and remain encrypted during use.