Policy/Procedure

Secure Messaging for Practitioners (MS-118)

Applies to: ☑ Hackley  ☑ All Sites  ☑ Mercy  ☑ Off-Site Services  ☑ Department Specific

Purpose

The purpose of these guidelines for practitioners is to advise mobile device users on appropriate methods of short content message communication (e.g., texting) that involves protected health information (PHI). In order to be in compliance with applicable laws and regulations, as well as internal policies and procedures, users should use Trinity Health’s-Sanctioned secure messaging application to access, receive, transmit or temporarily store PHI, including between and amongst physicians and other users. The Guidelines should be followed by users of all devices (including personally owned devices) that can be readily carried by an individual and are capable of receiving or transmitting digital information. (*Note: Use of e-mail is not governed by these Guidelines)

All other applicable MHM procedures, policies and standards, including the Health Insurance Portability & Accountability Act (HIPAA) Security Rule requirements, shall be adhered to while using a secure messaging application.

Guidelines

1. Mercy Health Muskegon permits the use of electronic text messages transmitted in a HIPAA compliant manner, either through the use of a Trinity Health-Sanctioned messaging application or by de-identification of personally identifiable information. Transmission of text messages containing PHI without the use of de-identification or the designated compliant messaging application is prohibited.

2. Secure texting will be used only for MHM professional business communications that include PHI for confidential purposes relating to treatment, payment, and health care operations.

3. Prior to communicating using devices to transmit PHI, practitioners shall obtain a secure messaging application.

4. Any device used for messaging PHI should initiate or enable a password protected lockout feature for the device’s primary screen. (i.e., the device, for example a smartphone, cannot be accessed unless a PIN or password is input).

5. Messages, including images and recordings, containing PHI may only be transmitted to and between Trinity Health-sanctioned secure messaging applications or electronic medical record...
applications sanctioned by MHM. Practitioners are prohibited from integrating a secure messaging application with any third-party applications, unless approved by MHM.

6. Messages, including images and recordings, that include PHI may only be taken and stored within the secure messaging application. They may not be stored outside of the secure messaging application (e.g., they may not be stored within the photo gallery of a smartphone). Taking a screen shot of information sent via the secure texting application is forbidden, as this represents a transfer of PHI to an unsecure medium.

7. PHI transmitted via secure message should be limited to the minimum amount of information necessary to accomplish the intended purpose of the disclosure.

8. If orders are sent by secure text, they will not be entered by hospital staff. Staff will call the ordering practitioner following the usual phone order process.

9. Practitioners taking images or recordings of a patient with a secure messaging application shall explain to the patient (1) why the image or recording is being taken and (2) that the image or recording will be transmitted to appropriate medical personnel in a secure manner.

10. Physicians and other members of the clinical care team, shall follow all clinical guidelines and use appropriate judgment when considering taking or attaching images related to patient care within a secure messaging application and to a secure message.

11. Physicians and other members of the clinical care team, should ensure (1) that images and recordings taken with a secure messaging application are of sufficient quality to accurately depict the subject thereof (e.g., proper lighting, orientation, scale, etc.) and (2) that they can be properly authenticated and identified.

12. Physicians and other members of the clinical care team should exercise appropriate judgment when considering whether to take and send an image or recording via a secure messaging application, taking into account the quality limitations of the secure messaging application, the timeframe in which the image or recording is needed, and whether the image or recording is needed for the care process.

13. In the event a device with the approved secure texting application installed is lost or stolen, the practitioner shall notify the MHM Service Desk immediately.

14. Each practitioner agrees to adhere to MHM's procedures for education, distribution and use of a secure messaging application as it relates to patient care.

15. All requirements and guidelines implemented by regulatory or accreditation entities, including but not limited to The Joint Commission, the Centers for Medicare and Medicaid Services (CMS), etc., shall be followed if requesting patient care via secure messaging. Practitioners have a responsibility to be aware of any guideline updates from these entities.
*For purposes of these Guidelines, mobile devices, PDAs, and smartphones are collectively referred to as "devices"*

Definitions:

- **Image** means a picture produced on an electronic display.
- **Message** means a transmitted or stored electronic communication, including texts, recordings and images.
- **Messaging** means sending, transmitting, receiving, uploading or downloading a message as defined in these Guidelines (*Note: E-mail is not included in this definition or governed by these Guidelines)*.
- **Mobile Device** means a device or workstation that can be physically removed from the worksite that may have the ability to use Wi-Fi, cellular networking, or other technologies that connect to the Internet or other data networks and include the following device types: laptops, Personal Digital Assistant (PDAs), handheld devices, digital tablets, smartphones, etc.
- **Password Protected** means secured with the use of a unique identifier or code.
- **Personal Digital Assistant (PDA)** means any small mobile hand-held device that provides computing and information storage and retrieval capabilities for personal or business use, often for keeping schedule calendars, note-entering, and address book information.
- **Protected Health Information (PHI)** means Individually Identifiable Health Information subject to the exceptions and exclusions in HIPAA.
- **Secure Message** means an electronic communication sent from one party to a recipient that ensures only the sender and recipient can access the communication.
- **Secure Messaging Application** means a software program is installed on a device that facilitates the transmission of encrypted text messages, images, and recordings.
- **Smartphone** means a wireless telephone set with special computer-enabled features.
- **Recording** means, but it not limited to, audio, voice, or video images that have been electronically captured and stored.
- **Treatment** means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.
- **Text** means the main body of electronic written matter.
- **Trinity Health-Sanctioned Messaging Application** means a software program that facilitates the transmission of secure messages, which may include PHI, and that has been approved for use by the Trinity Health Enterprise Information Security and the HIPAA/Privacy team. (*Note: For purposes of these Guidelines secure messaging applications sanctioned by another HIPAA Covered Entity are also permissible for use)*.
- **User** means and includes, but is not limited to, all Trinity Health/Mercy Health Muskegon colleagues, physicians, providers, medical, clinical, or technical staff, contractors, temporary staff, or external persons that perform a function for or on behalf of Mercy Health Muskegon or Trinity Health and that requires access to PHI.
RELATED PROCEDURES AND OTHER MATERIALS

- 45 C.F.R. Part 164 Subpart C – Security Standards for the Protection of Electronic Protected Health Information (i.e., the HIPAA Security Rule)

Review/Approval: Medical Executive Committee, May 9, 2017
Board of Trustees, June 22, 2017