
 <p><b>HAWAII HEALTH SYSTEMS</b> CORPORATION <i>"Quality Healthcare For All"</i></p> <p><b>PROCEDURE</b></p>	<b>Department:</b>  <p align="center"><b>Compliance</b></p>	<b>Policy No.</b>  <p align="center"><b>CMP 0057B</b></p>
	<b>Issued By:</b> <b>Audit &amp; Compliance Committee</b>	<b>Revision No.</b>  <p align="center">N/A</p>
	<b>Approved By:</b>    By: Linda Rosen, M.D., M.P.H. Its: CEO	<b>Effective Date:</b>  <p align="center">July 26, 2018</p> <b>Supersedes Policy:</b>  <p align="center">N/A</p> <b>Page:</b>  <p align="center">1 of 3</p>
<b>Subject:</b> <b>TEXTING PATIENT INFORMATION AMONG HEALTH CARE PROVIDERS AND STAFF MEMBERS</b>		

Last Review: 06/08/18; Next Review: 06/08/21

**I. PURPOSE:** To establish guidelines related to texting patient information among health care providers and staff members. Text messages are a form of informal communication that can be used to disseminate vital and time-sensitive information. This policy provides reasonable limitations to ensure text messages are used appropriately and in compliance with all applicable federal and state laws and regulations.

**II. DEFINITIONS:**

All capitalized terms used herein are defined in this Section II. Any other capitalized terms used in this policy are defined by the HIPAA Rules, applicable Hospital, Long-Term Care Facility, Critical Access Hospital, and Rural Health Clinic Conditions of Participation rules ("CoPs"), and CMS State Operations Manual Appendices A, PP, and W. All the definitions below are limited to the purposes of this policy.

"Clinical Staff Member" – means health care staff members involved in the care of the same patient and authorized to send and receive Text Messages. Clinical Staff Members shall include contracted or employed physicians or other health care providers and nursing staff members.

"Secure Platform" – an HHSC approved HIPAA compliant secure and encrypted means to send and receive Text Messages

"Texting" or "Text" – Texting means sending or receiving Text Messages on an HHSC approved Secure Platform.

"Text Message" – Text Messages are electronic communication between Clinical Staff Members and transmitted through a mobile device or computer system on an HHSC approved Secured Platform.

**III. PROCEDURES:**

- Text Messages shall be sent to only Clinical Staff Members authorized to use the Secure Platform. No Clinical Staff Members shall Text patients or any non-Clinical Staff Members.
- **\*\* Text Messages shall not be used for patient orders or order clarification.**
- The authorizing manager or supervisor for the respective Clinical Staff Member must submit a Corporate IT Security Access Request Form ("IT Access Form") to Corporate IT for each

respective Clinical Staff Member to use the Secure Platform and obtain training. Corporate IT and the Corporate Compliance Officer shall provide either in-person or written training materials to the authorizing manager or supervisor or, as requested by the facility, to the Clinical Staff Member. The IT Access Form is available at: to <http://sharepoint2013/sites/hhsc/corp/helpdesk/Document%20Library14/Corporate%20Office%20Network%20Access%20Request%20Form%20Master.pdf> or may be obtained by contacting the Corporate Office Help Desk by phone at (808) 733-4000 or toll free at (844) 459-0261.

- The authorizing manager or supervisor shall complete the following fields within the IT Access Form:
  - Requester Information
    - Enter the authorizing manager or supervisor's information.
    - The authorizing manager or supervisor must sign and date the IT Access Form.
  - End-User Information
    - Enter the Clinical Staff Member's information and indicate whether the Clinical Staff Member is a nurse or physician, etc.
  - Network, Email, Mobile, and Emerge Application Access
    - For authorized physicians or other authorized health care staff members: complete the Mobile Access column. Check "Cortext" and enter in the authorized physician's or other authorized health care staff member's email address.
    - For nurses or other health care staff members: complete the Network Access column. Check "Cortext-Desktop".
- **The authorizing manager or supervisor shall be responsible for informing Corporate IT of removing a Clinical Staff Member's authorization to use the Secure Platform in the event of the Clinical Staff Member's change of employment status, termination, or other event in accordance with HHSC's policies and procedures.**
- Clinical Staff Members shall send Text Messages to other Clinical Staff Members within the Secure Platform directory. Always confirm the recipient's name prior to sending any Text Message.
- Text Messages shall be concise and only include pertinent information. Avoid using shorthand or abbreviations. Before sending any Text Message, review the Text Message for accuracy, look for any auto-correction errors, confirm recipient.
- Two patient identifiers shall be used in the Text Message that refers to the respective patient. The two patient identifiers shall include the patient's full name and one of the following: date of birth, medical record number, encounter number, age, or sex.
- Check Text Message status to confirm delivery and receipt of the Text Message.
- Texting of pictures or images to another Clinical Staff Member is permitted only if the pictures or images are taken on an HHSC approved device in accordance with the respective HHSC Facility's policies and procedures. No mobile device shall be used to take any patient pictures or images.
- Any Text Message that contains the following information shall be charted in the respective patient's medical record in accordance with the respective HHSC Facility's policies and procedures:

- Information to justify an admission and continued hospitalization,
  - Information to support patients' diagnosis, that describes patients' progress and response to medications and services,
  - Information that describes changes in the patients' condition,
  - Information that describes any patient related complication, and
  - Any other information that should be charted in the patients' medical record.
- Immediately report any Text Messages that are sent to an unintended or wrong individual to Corporate Compliance.
  - "Screenshots" or taking pictures of any Text Message on the Secure Platform is prohibited.
  - Clinical Staff Members shall not share Secure Platform usernames or passwords, or both, disable or alter any security measures within the Secure Platform, or use the Secure Platform in any manner that violates HHSC's policies or unrelated to the authorized or permitted use, or both. Clinical Staff members shall exit or log out of the Secure Platform after each use.
  - Clinical Staff Members authorized to use their personal mobile devices are responsible for the physical security of those devices at all times. In the event a mobile device becomes lost, stolen, or retired ("Incident"), the Clinical Staff Member shall immediately report the Incident to the HHSC Help Desk by phone at (808) 733-4000 or toll free at (844) 459-0261. Immediate shall mean within 30 minutes of becoming aware of the Incident.
  - Corporate Compliance, with the assistance of Corporate IT, shall conduct monthly audits of the Secure Platform and any Text Message sent or received.

**IV. APPLICABILITY:** All HHSC facilities and Clinical Staff Members.

**V. AUTHORITY:** 45 C.F.R. Parts 160, 162, and 164, 42 C.F.R. Parts 482, 483, 485 Subpart F, and 491; Telephone Consumer Protection Act of 1991, codified at 47 U.S.C. § 227 ("TCPA"); FCC TCPA Omnibus Declaratory Ruling and Order; available at <https://www.fcc.gov/document/tcpa-omnibus-declaratory-ruling-and-order>; HHSC Corporate Compliance Program CMP 0001A; HHSC policies: CMP 020A (HIPAA Privacy and Security Policy and Practices Requirements); CMP 17A (Policy for Use of Social Networking and Other Electronic Media); CMP 008A (Retention of Records); CMP 0026A (Sanctions); CMP 0100A (Nondiscrimination); ITD 0000A (Definitions), ITD 0005A (Information Systems Access), ITD 0008 (Termination). All such statutes, regulations, and HHSC policies may be amended from time to time.

**VI. REFERENCES:** CMS Memorandum S&C 18-10-ALL regarding Texting of Patient Information among Healthcare Providers dated December 28, 2017, available at: <https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertificationGenInfo/Downloads/Survey-and-Cert-Letter-18-10.pdf>; Clarification from The Joint Commission titled "Use of Secure Text Messaging for Patient Care Orders Is Not Acceptable" dated December 2016, available at: [https://www.jointcommission.org/assets/1/6/Clarification\\_Use\\_of\\_Secure\\_Text\\_Messaging.pdf](https://www.jointcommission.org/assets/1/6/Clarification_Use_of_Secure_Text_Messaging.pdf); *ACA International v. FCC*, 885 F.3d 687, 710-14 (D.C. Cir. 2018) (upholding FCC TCPA Omnibus Declaratory Ruling and Order pertaining to healthcare providers).

CMP 0057A

**VII. ATTACHMENTS:** Reference Guide.