
 <p>HAWAII HEALTH SYSTEMS CORPORATION <i>"Quality Healthcare For All"</i></p> <p>POLICY</p>	Department: Compliance	Policy No. CMP 0057A
	Issued By: Audit & Compliance Committee	Revision No. N/A
	Approved By:  HHSC Board of Directors By: Donna McCleary, M.D. Its: Secretary/Treasurer	Effective Date: July 26, 2018
		Supersedes Policy: N/A
Subject: TEXTING PATIENT INFORMATION AMONG HEALTH CARE PROVIDERS AND STAFF MEMBERS	Page: 1 of 3	

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. **POLICY:**

A. In accordance with the HIPAA Rules, Clinical Staff Members may send Text Messages to other Clinical Staff Members on the Secure Platform. Only authorized physicians and other health care staff members may send and receive Text Messages on their personal mobile devices, provided that the Secure Platform is installed on the personal mobile device prior to any Texting. No Clinical Staff Members shall Text outside of the Secure Platform. No Clinical Staff Members shall Text patients or any non-Clinical Staff Members.

B. In compliance with the relevant CoPs, **Texting of patient orders and order clarifications are prohibited.**

- C. Text Messages are not automatically entered as part of the patients' permanent medical record.
- D. 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.
- E. All Text Messages are the sole property of HHSC. HHSC has the absolute right to access any Text Message for purposes that include, but are not limited to: retrieval, monitoring, and auditing to ensure Text Messages are in compliance with this policy and all applicable laws and regulations. HHSC shall store and archive all Text Messages in accordance with HHSC's Retention of Records policy.
- F. In compliance with HHSC's Corporate Compliance Program and Nondiscrimination policy, Texting shall be conducted in a professional, ethical, and lawful manner.
- G. Text Messages shall not replace direct communication between Clinical Staff Members and may not be the sole method of communication.
- H. Usage of Texting shall be in accordance with the corresponding HHSC Corporate Office policies and procedures and the respective HHSC Facility's policies and procedures.
- I. 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. For purposes of this policy, immediate shall mean within 30 minutes of becoming aware of the Incident.
- J. In accordance with HHSC's policies, 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. Any Clinical Staff Members who violate this policy shall be subject to appropriate disciplinary action in accordance with the respective HHSC Facility's policies and procedures and any applicable collective bargaining agreement or HHSC Human Resources and Civil Service System Rules.

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; *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 0057B

- VII. ATTACHMENTS:** Reference Guide.