DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop C2-21-16
Baltimore, Maryland 21244-1850

Center for Clinical Standards and Quality/Quality, Safety & Oversight Group

Ref: QSO-24-05-Hospital/CAH

DATE: February 8, 2024

TO: State Survey Agency Directors

FROM: Director, Quality, Safety & Oversight Group (QSOG)

SUBJECT: Texting of Patient Information and Orders for Hospitals and CAHs

Memorandum Summary

- **Texting patient information and the texting of patient orders among members of the health care team is permissible, if accomplished through a HIPAA compliant secure texting platform (STP) and in compliance with the Conditions of Participation (CoPs).**
- **Computerized Provider Order Entry (CPOE) continues to be the preferred method of order entry by a provider.**

Background:

On January 5, 2018, CMS released QSO-18-10-Hospital, CAHs Revised memorandum, "Texting of Patient Information among Healthcare Providers in Hospitals and Critical Access Hospitals (CAHs)," which acknowledged that the use of texting had become an essential means of communication among hospital and CAH healthcare team members; however, CMS noted the practice of texting patient orders from a provider to a member of the care team would not be compliant with the CoPs, citing concerns with record retention, privacy, confidentiality, security, and the integrity of existing systems at that time.

When CMS developed the 2018 guidance, most hospitals and CAHs did not have the ability to use secure texting platforms to incorporate these messages into the medical record.

Discussion:

The hospital and CAH medical record CoPs at 42 CFR 482.24 and 485.638, respectively, require among other things that inpatient and outpatient medical records be accurately written, promptly completed, properly filed and retained, and accessible. Also, the hospital must use a system of author identification and record maintenance that ensures the integrity of the authentication and protects the security of all record entries. These requirements do not specify a specific method or system that must be used for author identification and record maintenance.

CPOE continues to be the preferred method of order entry by a provider, but we recognize that alternatives also exist now, as well as significant improvements in the encryption and application interface capabilities of texting platforms to transfer data into electronic health records (EHR).

CMS has held that a physician or advanced practice provider should enter orders into the medical record via a handwritten order or CPOE. An order entered via CPOE, and immediately downloaded into the hospital's or CAH's EHR system, is permitted under the requirements because the order is dated, timed, authenticated, and promptly placed in the medical record.

To comply with the CoPs, all providers must utilize and maintain systems/platforms that are secure and encrypted and must ensure the integrity of author identification as well as minimize the risks to patient privacy and confidentiality, as per the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations. Providers should implement procedures/processes that routinely assess the security and integrity of the texting systems/platforms that are being utilized to avoid negative outcomes that could compromise the care of patients.

CMS expects that providers choosing to incorporate texting of patient information and orders into their EHR will implement a platform that meets the requirements of the HIPAA Security Rule[1] and the HITECH Act Amendment 2021[2] as well as the CoPs.

Contact:
For questions or concerns relating to this memorandum, please contact QSOG_Hospital@cms.hhs.gov.

Effective Date:
Immediately. Please communicate to all appropriate staff within 30 days.

/s/
David R. Wright
Director, Quality, Safety & Oversight Group

Resources to Improve Quality of Care:
Check out CMS's new Quality in Focus interactive video series. The series of 10–15 minute videos are tailored to specific provider types and intended to reduce the deficiencies most commonly cited during the CMS survey process, like infection control and accident prevention. Reducing these common deficiencies increases the quality of care for people with Medicare and Medicaid.
Learn to:

- *Understand surveyor evaluation criteria*
- *Recognize deficiencies*
- *Incorporate solutions into your facility's standards of care*

See the Quality, Safety, & Education Portal Training Catalog, and select Quality in Focus.

[1] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164.
[2] HITECH Act Amendment 2021 requires that the Department of Health and Human Services (HHS) consider whether a covered entity or business associate has "adequately demonstrated" it had, for not less than the previous 12 months, "recognized security practices" in place when making certain determinations under the HIPAA Security Rule.