Akin®

CMS Revises Policy on Texting Patient Orders

March 15, 2024

Reading Time : **3 min**

By: Kelly M. Cleary, Jo-Ellyn Sakowitz Klein, Oluwaremilekun O. Mehner

On February 8, 2024, the Centers for Medicare and Medicaid Services (CMS) released a memorandum from the Quality, Safety & Oversight Group (QSOG) updating its 2018 guidance on texting patient information among healthcare providers in hospitals and critical access hospitals (CAHs) to permit the texting of patient orders among members of a patient's healthcare team if certain conditions are met.[1]

In its 2018 guidance, CMS stated that texting patient orders from a provider to a member of the patient's care team would not be compliant with the Medicare Conditions of Participation[2] (CoPs). CMS noted particular concerns with record retention, privacy, confidentiality, security, and system integrity. Instead, CMS required that provider orders be either handwritten into the medical record or entered through the Computerized Provider Order Entry (CPOE) and then promptly placed into the medical record.

In updating the guidance, CMS notes that in 2018, most hospitals and CAHs did not have the ability to use secure texting platforms to incorporate orders into the medical record. CMS stated that though CPOE remains the agency's preferred method of order entry, suitable alternatives exist, and noted that there have been significant improvements in encryption and application programming interface (API) capabilities of texting platforms to transfer data into electronic health records (EHR).

In light of this, CMS determined that healthcare providers in hospitals and CAHs can text patient orders if accomplished through a HIPAA[3]-compliant, secure texting platform (STP) and in compliance with the CoPs. CMS stated it expects providers choosing to incorporate

texting of patient information and orders into their EHR will use platforms that meet the requirements of the CoPs, the HIPAA Security Rule,[4] and also the 2021 amendment to the Health Information Technology for Economic and Clinical Health Act of 2009[5] (HITECH Amendment 2021).

The hospital and CAH CoPs on medical records require, among other things, that medical inpatient and outpatient medical records be "accurately written, promptly completed, properly filed and retained, and accessible."[6] 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.[7] The CMS memorandum specifies: "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."

CMS further notes that providers using STPs should implement procedures/processes that routinely assess the security and integrity of the system or platform "to avoid negative outcomes that could compromise the care of patients."

If you have any questions, please contact a member of the Akin health regulatory or cybersecurity, privacy and data protection teams.

---

1 *See* Center for Clinical Standards and Quality/Quality, Safety & Oversight Group (Centers for Medicare and Medicaid Services), *Texting of Patient Information and Orders for Hospitals and CAHs, Ref: QSO-24-05-Hospital/CAH*, (Feb. 8, 2024) *available at* https://www.cms.gov/files/document/qso-24-05-hospital-cah.pdf.

2 *See, e.g.*, 42 C.F.R. §§ 482.24 and 485.638.

3 As used here, "HIPAA" refers to the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act of 2009, together with their implementing regulations codified at 45 C.F.R. Parts 160 to 164.

4 In effect since 2005, the HIPAA Security Rule established national standards to protect individuals' electronic protected health information that is created, received, maintained, or transmitted by a covered entity or business associate. At its core, the HIPAA Security Rule *requires* reasonable and appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. *See* 45 C.F.R. Part 160; 45 C.F.R. 164 Subparts A and C.

5 HITECH Amendment 2021 established a mechanism under which entities subject to HIPAA that *voluntarily* implement certain recognized security practices (RSPs) could face milder repercussions in federal enforcement actions related to HIPAA Security Rule violations, provided they can "adequately demonstrate" the RSPs were in place for at least twelve months. *See* 42 U.S.C. § 17941 (emphasis added).

6 42 C.F.R. § 482.24(b).

7 *See id.*

Categories

Cybersecurity, Privacy & Data Protection | Privacy & Data Protection