DECEMBER 28, 2017

CMS PROHIBITION ON TEXTING? EVALUATING NEXT STEPS FOR YOUR ORGANIZATION

For an update to this article, please click here.

As stated in our previous blog, while there has been **no official** guidance from CMS regarding a broad prohibition on the texting of protected health information ("PHI"), there has been significant discussion in industry circles about CMS's recently stated position against texting PHI. As reported in the Health Care Compliance Association article - CMS Says No Texting Allowed, Citing HIPAA, CoP; Lawyer: 'Like Going Back to Dark Ages' [paywall] - CMS has apparently taken the position with certain hospitals that no texting of PHI, even via secure texting platforms, is permissible. As a result, health care providers and health-related entities are left to operate in a gray area with potentially significant operational and financial implications but a lack of clarity regarding the exact risk.

Apparently, CMS is basing the prohibition against texting PHI on two concerns. First, CMS is concerned that such texts will not comply with the HIPAA Security Rule, 45 CFR Parts 160 and 164. CMS is also reportedly concerned that text messages cannot or will not be recorded in a manner that meets the documentation requirements of Conditions of Participation 42 C.F.R. § 482.24 ("CoP") for accurate and complete medical records.

Use of texts to transmit PHI has a long and troubled history. In 2011, The Joint Commission advised providers that text messaging of patient information was prohibited. In May 2016, that prohibition was lifted, and CMS and The Joint Commission provided guidance that all health care organizations should have policies prohibiting the use of **unsecure** text messaging of PHI (e.g., standard SMS messaging provided by the mobile services provider) but that secure text messaging was permissible.

- The Joint Commission May 2016 guidance provided that health care organizations implementing secure text messaging platforms should ensure the platform includes the following:
  - Secure sign-on process;
  - Encrypted messaging;
  - Delivery and read receipts;
  - Date and time stamp;
  - Customized message retention time frames; and
  - Specified contact list for individuals.

- However, subsequent clarifying guidance was issued in December 2016. The joint guidance issued by The Joint Commission and CMS in December 2016 prohibited texting physician orders but did not forbid more general uses of secure texting platforms.

Presently, many health care organizations are seeking, ready to implement or already using a secure texting platform. Depending upon your organization's scenario, we offer the following approaches to consider.

Scenario 1: My organization already has a secure texting solution.

- As there is no official prohibition on texting PHI at this point in time, immediately shutting down the texting solution is not necessarily required if your organization is in compliance with HIPAA and the CoP documentation requirements.
- Confirm that your organization reviewed the security of the secure texting platform pursuant to HIPAA Security Rule standards, including the addressable and required administrative, physical and technical safeguards, and documented that assessment. If the review was performed but not documented at that time, document it now.

- Confirm that the texting solution was configured at implementation in a manner that ensures the highest possible security.
- Confirm that your organization has policies and procedures in place for appropriate documentation in the patient medical record of those text communications that must be documented and ensure compliance with those policies and procedures.
- Conduct training to reinforce the appropriate use of texting of PHI under your policies.
- Remain aware that significant changes may have to be made if and when official guidance is issued.

Scenario 2: My organization has signed a contract for a secure texting solution, but it is not yet live.

- If you have not already done so, review the security of the secure texting platform pursuant to HIPAA Security Rule standards and document that assessment, including the addressable and required administrative, physical and technical safeguards.
- Develop policies and procedures for appropriate documentation of the secure text messages in the medical record part of the implementation.
- If economically and contractually feasible, consider delaying or slowing the implementation for a few weeks in order to respond to official guidance that may be issued.

Scenario 3: My organization is in the process of procuring a secure texting solution.

- Continue to vet texting solutions. Assess the security of secure texting platforms pursuant to the HIPAA Security Rule and industry standards. Document the assessment, including the addressable and required administrative, physical and technical safeguards.
- Place on hold final selection in order to respond to any official guidance that may be issued.
- Consider negotiating a contractual provision permitting an early termination in the event secure texting of PHI is prohibited.

Finally, all organizations that allow some form of texting of PHI should perform a risk assessment of the organization's use of texting. The assessment should thoroughly evaluate the overall benefits versus the risks and address communications regarding patient care. If your organization does not permit texting, verify that your organization's policy is adequately enforced.

We recommend consulting legal counsel and your organization's internal stakeholders to determine the best approach to this issue for your organization.

For more information, please contact:

- Jeff Short at (317) 977-1413 or jshort@hallrender.com;
- Melissa Markey at (248) 740-7505 or mmarkey@hallrender.com;
- Liz-Callahan-Morris at (248) 457-7854 or ecallahan@hallrender.com;
- Charise Frazier at (317) 977-1406 or cfrazier@hallrender.com;
- Patricia Connelly at (317) 429-3654 or pconnelly@hallrender.com; or
- Your regular Hall Render attorney.