Health Law Alert: HIPAA Confusion on Texting Swirls, as Preliminary Audit Results Suggest Widespread Noncompliance

January 8, 2018

In December 2017, reports emerged that the Centers for Medicare and Medicaid Services (CMS) had announced a strict "no texting" ban for providers. The supposed ban came not in the form of regulations, revisions to CMS Manuals or other formal guidance, but rather in emails sent to several hospitals from the CMS body tasked with oversight of provider Conditions of Participation (COPs). A formal memorandum was published at the end of 2017 that tempers the supposed restriction. All of this comes on the heels of the Office for Civil Rights (OCR) releasing preliminary results of Phase 2 of the HIPAA Audit Program. The results are very negative. Because the point of the current auditing initiative is to aid in structuring OCR's permanent HIPAA Audit Program, providers are not likely to see relaxation on enforcement any time soon.

A New "No Texting" Rule?

Reports emerged in early December that several hospitals had received emails from CMS indicating a new position regarding text messaging. These emails suggested that no texting of protected health information (PHI) was permitted, even if secure texting solutions were used. The rationale was because the "receiving or sending phones may not always be secure and encrypted, the privacy of the patient and his/her personally identifiable information (PII) cannot be guaranteed, and the sender or receiver cannot always be identified potentially exposing PHI/PII. In addition, the information contained in the text messages would be required to be entered into the patient's medical record and available for retrieval." The position emerged from CMS' Survey & Certification Group and was based at least in part on Medicare COP requirements for hospitals. Many providers were shocked by this announcement, considering that OCR (which is, of course, charged with HIPAA oversight) had not itself taken this position.

CMS Survey & Certification Memorandum Tempers the Rule (Somewhat).

On Dec. 28, 2017, the Survey & Certification Group issued a memo to state survey agency directors that appears to take a more nuanced position (the "Memo"). The Memo made the following points about text messaging:

1. Medicare COPs and Conditions for Coverage do not permit "texting orders from a provider to a member of the care team". Electronic orders via computerized provider order entry (CPOE) are permitted and are in fact the "preferred method." Use of CPOE can meet COPs as long as there is an "immediate download" into the provider's electronic health record.

2. CMS took a different position than the strict "no texting" position discussed above. The agency explained that it recognized that texting "has become an essential and valuable means of communication among [healthcare] team members." However, CMS noted that this does not allow the use of any text messaging application. In order to comply with COPs/CFCs, providers must use ***secure and encrypted*** messaging systems or platforms. This is based on HIPAA and the COP/CFC requirements. In addition, providers are expected to implement procedures and processes to routinely assess the security and integrity of their messaging systems or platforms.

HIPAA Audit Program Results: Not a Good Report Card

Although CMS' position on texting may be a surprise, the increased focus on HIPAA and enforcement is not. OCR has been ramping up HIPAA enforcement through the HIPAA Audit Program since 2011. The preliminary results of Phase 2 of this program were recently released and the results, which were alarmingly negative, will likely lead to even more aggressive enforcement by OCR.

The HIPAA Phase 2 Audit Program involved 166 covered entity audits and 41 business associate audits. Health care providers (as opposed to plans or clearinghouses) represented the vast majority (over 90%) of covered entities audited.

In the Midwest region, 38 covered entities and 15 business associates were audited. While these numbers may not seem particularly high, OCR conducted more covered entity and business associate audits in the Midwest than in any other part of the country. The audits involved reviewing compliance with various aspects of the HIPAA Privacy, Security and Breach Notification regulations. The following areas were among those reviewed by OCR:

- Notice of Privacy Practices requirements;

- Patient rights to access their own PHI;
- Documentation, timeliness and content of breach notifications;
- Security Rule risk analysis; and
- Security Rule risk management.

The results suggest significant problems. OCR used a scale of 1 to 5 to judge results, with "1" or "2" indicating full or substantial compliance and "4" or "5" signifying "negligible efforts" or no "evidence of [a] serious attempt to comply." A designation of "3" is hardly positive, indicating that the results "minimally address audited requirements," but "implementation is inadequate" or reflects a "misunderstanding of requirements."

Most organizations received very poor scores. For example, 67% of the organizations evaluated received "inadequate" or worse scores on meeting content requirements for breach notification. Further, 65% of organizations were "inadequate" or worse on the content requirements for their notices of privacy practices. Security Rule compliance was even worse. The results indicated that a stunning 83% of organizations did not perform an appropriate Security Rule risk analysis and 94% of the total did not establish or maintain Security Rule risk management plans. Even something as straightforward and longstanding as Privacy Rule requirements on patients having access to their own PHI showed very problematic results, with 89% failing to meet requirements.

The results should raise alarm bells for health care providers and their business associates. It demonstrates that not only is OCR taking an aggressive stance on HIPAA compliance, but also that many providers are failing to meet their standards. All of this suggests that HIPAA compliance will remain a key issue for providers and business associates in 2018.

If you have questions about HIPAA or other federal and state privacy and security requirements, please contact Jesse Berg at jesse.berg@lathropgpm.com (612.632.3374), Tim Johnson at tim.johnson@lathropgpm.com (612.632.3208), or Julia Reiland at julia.reiland@lathropgpm.com (612.632.3280).