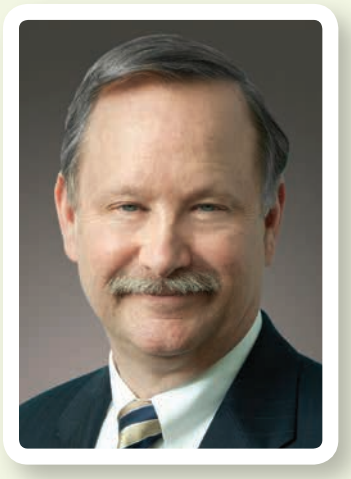
Key Legal Issues for Medical Practices: Provider Tips for Emailing and Texting with Patients in Compliance with HIPAA

By James B. Riley, Kimberly J. Kannensohn and Paige Dowdakin



At the 2016 RPA Annual Meeting, the topic of electronic communications with patients in the 21st century was addressed and we thought that a follow-up article reiterating some of the key considerations in this area of HIPAA would be worth emphasizing. The safest way to communicate with patients in compliance with the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (HIPAA) is in person or via telephone. However, given the efficiencies associated with electronic communication and the extent to which it is now relied upon by providers and patients in the delivery and receipt of health care, health care providers often communicate patients' protected health information, or PHI, electronically. If a physician or other provider decides to engage in such communications, careful attention must be paid to the requirements of HIPAA and the policies and procedures of the physician's practice, clinic or institution.[1]

Minimizing the Risk of a HIPAA Violation in Communicating with Patients via Email

While health care providers are free to adopt policies restricting the use of email in patient communications, HIPAA itself does not prohibit the transmission of PHI by email. However, transmitting PHI via an unsecure, unencrypted email creates a risk that the PHI will be accessed or disclosed in an unauthorized manner, resulting in a breach under HIPAA.[2] There are a number of ways that a physician or other provider may minimize the risk of a breach, as well as the risk of a patient complaint in connection with the emailing of PHI.

As a threshold matter, physicians or other providers should not communicate with patients by email without the patient's express written consent. The principal objective of HIPAA is to protect a patient's privacy rights in connection with his or her health information, and, thus, if a patient has indicated that he or she only wants to receive such information via telephone or in person, a physician or other provider should not, under any circumstances, communicate with that patient via email. Moreover, if a patient has not imposed such restrictions, but later objects to communications received from the provider via email, the presence in the file of a written consent from the patient regarding electronic communications will protect the provider in the event of a patient complaint, Office for Civil Rights (OCR) investigation, or other government action. In connection with procuring any such consent, the provider or practice should notify the individual about the risks that the information in the email could be read by a third party.[3]

The most effective means of avoiding a breach in connection with the transmission of PHI via email is to encrypt the communication. On August 24, 2009, HHS published an interim final rule for breach notification in the case of a breach of unsecured PHI under HIPAA. The interim rule, which implements provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), provides the equivalent of a safe harbor for "secured PHI" which has been rendered unreadable, unusable, or indecipherable to unauthorized individuals through encryption using a methodology specified under the HITECH Act.[4] If a covered entity discovers an unauthorized use or disclosure of "secured PHI," the covered entity will not be required to comply with the breach notification requirements under HIPAA because the information is not considered unsecured PHI subject to HIPAA's breach reporting requirements.[5] Accordingly, if possible, providers should encrypt email communications containing PHI in accordance with the encryption safe harbor.

If encryption is not possible, providers should implement the following safeguards to minimize the risk of a breach of PHI:

1. Providers should use and confirm the email address specifically provided by the patient for that purpose;
2. Providers should avoid including PHI in the subject line and review all attachments and forwarded emails to ensure that they do not contain the PHI of other patients;
3. Providers should double check the recipients on any email before sending PHI to ensure that the email address is accurate and to ensure that there are no unintended recipients;
4. Providers should only transmit the minimum amount of PHI necessary for effective communication with the patient (e.g., do not attach the entire visit record if the patient is inquiring about a single laboratory report) and avoid sending sensitive PHI (HIV/AIDS, substance abuse, mental health, etc.);
5. Emails should include a notice of confidentiality, which instructs unintended recipients of the steps they must take upon receipt of the misaddressed email, including notifying the sender, ensuring that the email is not forwarded to anyone, and deleting all copies of the email; and
6. Providers and practices should develop a written policy regarding communicating with patients via email and train all workforce members regarding the policy.

On January 25, 2013, the OCR published its final rule modifying the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the HITECH Act.[6] This final rule, commonly referred to as the "Omnibus Rule," clarified that covered entities are not responsible for a breach notification under HIPAA in the event that unauthorized access of PHI occurs as a result of sending an unencrypted email based on an individual's request. As set forth in the Omnibus Rule, if individuals are "notified of the risk, and still prefer unencrypted email, they have the right to receive [the unencrypted email in accordance with their request], and covered entities are not responsible for unauthorized access of protected health information while in transmission to the individual based on the individual's request." Nonetheless, to minimize the risk of unauthorized access and to avoid being placed in a defensive position, providers should always take the above-referenced precautions with respect to the transmission of PHI through unencrypted email.

Safe Disposal of Emails Containing PHI

HIPAA compliance efforts do not end once the provider hits "send." Emails which remain on computers and other devices, or emails which have been printed, remain at risk for re-disclosure. The HIPAA Privacy and Security Rules do not mandate a single method for the disposal of PHI. Providers and practices that transmit PHI via email should nonetheless adopt policies regarding the destruction of PHI and should also train workforce members regarding those policies. Factors to consider when developing these policies include:

(1) whether the PHI is in electronic or hard copy form;

(2) whether the PHI contains social security numbers or other sensitive financial information; and

(3) the type and amount of PHI disclosed.

Providers and practices should also review their particular environment in developing and implementing policies and procedures, so that such

---

1 State law requirements regarding electronic communications should also be reviewed, as they may differ from HIPAA.
2 Unsecure, unencrypted emails may be intercepted and may be copied onto and remain on the servers that transmit the email between the sender and recipient.
3 *See* 78 Fed. Reg. 5566, 5634 (Jan. 25, 2013).
4 *See* 74 Fed. Reg. 42740 (Aug. 24, 2009). Under the interim rule, electronic PHI is considered encrypted as specified in the HIPAA Security Rule by the use of two elements: a process or key that is kept confidential and an algorithm to transform data into a form where there is a low probability that the data can be given meaning without the use of that process or key. *Id*. The interim rule specifies encryption processes that have been tested by the National Institute of Standards and Technology (NIST) for each of the following categories of data: data in motion, data at rest, data disposed, and data in use.
5 State reporting requirements may differ from HIPAA, and, accordingly, should always be reviewed in the event of a breach of PHI.
6 *See* supra note 3.

policies and procedures are appropriately tailored to their physical setting and capabilities.

Policies regarding the destruction of PHI should incorporate instructions for actual destruction methods based on the type of PHI. Electronic media, such as CDs, DVDs, flash drives, and other devices such as portable phones should be cleared and stripped of electronic PHI before being recycled or reused. Software and hardware that contains PHI may be cleared using products to overwrite media with non-sensitive data, purged by degaussing or exposing the media to a strong magnetic field, or otherwise destroyed. E-mail printouts should not be placed in dumpsters or recycling bins that are accessible by the public or other unauthorized individuals. Proper disposal methods of printed PHI may include shredding, burning, or otherwise rendering PHI unreadable and unable to be reconstructed. If providers use third party vendors to destroy PHI, providers should retain all PHI in a safe, locked area prior to its destruction.

Texting PHI to Patients

Text messaging is not prohibited under HIPAA, but like other forms of communication it involves some level of risk of unauthorized disclosure. As a result, some practices and institutions prohibit or strongly discourage physicians or other providers from texting PHI. Traditional text messaging creates risk under HIPAA by virtue of how it is generated, transmitted, stored, and viewed. For example, text messages are transmitted in clear text without any level of authentication, meaning that anyone who has access to the device may have access to all text messages on the device without needing a password. PHI may also remain stored on wireless carrier servers, depending on the carrier's retention policies, and may be intercepted while in transit. Finally, text messages may reside on a mobile device indefinitely, where the information can be exposed to unauthorized third parties due to theft, loss, or disposal of the device.

Due to the inherent risks of disclosure with regard to transmitting PHI via text message, the best approach for practices and institutions that allow PHI to be sent via text message is to utilize encryption technology. If encryption technology is not viable or has not yet been obtained by a practice or institution, physicians or other providers should consider relying on alternate means to communicate with patients.[7]

As with email messaging, if a patient insists on receiving PHI via a text message, and your practice or institution does not have a policy prohibiting it, it is important to ensure that the patient has provided advanced written consent to the transmission of PHI via text message. Finally, providers and practices should institute the same processes and safeguards specified above for emailing PHI when transmitting PHI through text messaging.[8] ■

Mr. Riley is a partner and immediate past Chair of the McGuireWoods' Healthcare Department. Ms. Kannensohn is a partner in the McGuireWoods Healthcare Department and Ms. Dowdakin is an associate in the McGuireWoods Healthcare Department.

Editor's Note: *This article is for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue or problem. The opinions expressed at or through this article are the opinions of the individual authors and may not reflect the opinions of the firm or any individual attorney.*

7 Note that appointment reminders sent via text message may also constitute PHI.

8 The OCR is currently commencing Phase Two of its HIPAA Audit Program. Office for Civil Rights, "OCR Launches Phase 2 of HIPAA Audit Program," available at **http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/index.html** (Mar. 21, 2016). The OCR has explained that every "covered entity and business associate is eligible for an audit. These include covered individual and organizational providers of health services; health plans of all sizes and functions; health care clearinghouses; and a range of business associates of these entities." Office for Civil Rights, "HIPAA Privacy, Security, and Breach Notification Audit Program," available at **http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html#who**.