Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

E-mailing and Texting PHI: Beware HIPAA

Insight — March 18, 2025

The HIPAA Privacy and Security Rules require covered entities (including healthcare providers and health plans) and their business associates to protect patient information stored or transmitted electronically, including protected health information ("PHI") sent in unsecure texts or e-mails.

E-mails and Texts *to* Patients. The HIPAA Privacy Rule not only allows but requires covered entities to communicate with patients via e-mail or text if requested by the patient (*see* 45 CFR § 164.522(b)), but the Privacy Rule requires covered entities to implement appropriate safeguards when e-mailing or texting e-PHI to patients. The Office for Civil Rights ("OCR") explained:

> The Privacy Rule allows covered health care providers to communicate electronically, such as through e-mail, with their patients, provided they apply reasonable safeguards when doing so. (See 45 CFR § 164.530(c)). For example, certain precautions may need to be taken when using e-mail to avoid unintentional disclosures, such as checking the e-mail address for accuracy before sending or sending an e-mail alert to the patient for address confirmation prior to sending the message. Further, while the Privacy Rule does not prohibit the use of unencrypted e-mail for treatment-related communications between health care providers and patients, other safeguards should be applied to reasonably protect privacy, such as limiting the amount or type of information

> disclosed through the unencrypted e-mail. In addition, covered entities will want to ensure that any transmission of electronic protected health information is in compliance with the HIPAA Security Rule requirements at 45 CFR Part 164, Subpart C.

(OCR FAQ dated 12/15/08, available at http://www.hhs.gov/ocr/privacy/hipaa/faq/health_information_technology/570.html).

The HIPAA Security Rule generally requires covered entities and business associates to "[i]mplement technical security measures to guard against unauthorized access to [e-PHI] that is being transmitted over an electronic communications network." (45 CFR § 164.312(e)(1)). Encryption is an addressable implementation standard, meaning that the covered entity or business associate must encrypt the e-PHI if it determines that doing so is "reasonable and appropriate" and, if not, the covered entity or business associate must "(1) Document why it would not be reasonable and appropriate to [encrypt the data]; and (2) Implement an equivalent alternative measure if reasonable and appropriate." (*Id*. at § 164.312(e)(2)). Again, the OCR explained:

> The Security Rule does not expressly prohibit the use of email for sending e-PHI. However, the standards for access control (45 CFR § 164.312(a)), integrity (45 CFR § 164.312(c)(1)), and transmission security (45 CFR § 164.312(e)(1)) require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to e-PHI. The standard for transmission security (45 CFR § 164.312(e)) also includes addressable specifications for integrity controls and encryption. This means that the covered entity must assess its use of open networks, identify the available and appropriate means to protect e-PHI as it

> is transmitted, select a solution, and document the decision. The Security Rule allows for e-PHI to be sent over an electronic open network as long as it is adequately protected.

(OCR FAQ available at http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2006.html, emphasis added).

Thus, to communicate e-PHI to patients via e-mail or text, the covered entity or business associate has two options:

1. Secure the Transmission. The covered entity or business associate may encrypt the e-PHI and/or use other appropriate means to ensure that the e-PHI is secure. As HHS explained:

> In this environment of more online access and great demand by consumers for near real-time communications, you should be careful to use a communications mechanism that allows you to implement the appropriate Security Rule safeguards, such as an email system that encrypts messages or requires patient login, as with a patient portal. If you use an EHR system that is certified under ONC's 2014 Certification Rule, your EHR should have the capability of allowing your patients to communicate with your office through the office's secure patient portal. If you attest to Meaningful Use and use a certified EHR system, you should be able to communicate online with your patients. The EHR system should have the appropriate mechanisms in place to support compliance with the Security Rule. You might want to avoid other types of online or electronic communication (e.g.,

> texting) unless you first confirm that the communication method meets, or is exempt from, the Security Rule.

(*HHS Guide to Privacy and Security of Electronic Health Information* at p.31, available at http://www.healthit.gov/providers-professionals/guide-privacy-and-security-electronic-health-information).

2. Warn the Patient. If the network or means of communication is not secure and/or the e-PHI is not encrypted, a covered entity or business associate may still communicate with patients via e-mail or text so long as they warn the patient in advance. In its Omnibus Rule commentary, HHS confirmed:

> covered entities are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email. We disagree that the "duty to warn" individuals of risks associated with unencrypted email would be unduly burdensome on covered entities and believe this is a necessary step in protecting the protected health information. We do not expect covered entities to educate individuals about encryption technology and the information security. Rather, we merely expect the covered entity to notify the individual that there may be some level of risk that the information in the email could be read by a third party. If individuals are notified of the risks and still prefer unencrypted email, the individual has the right to receive protected health information in that way, 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.

(78 FR 5634).

E-mails and Texts *from* Patients. The foregoing rules apply to e-mails or texts by the covered entity or business associate to patients; the same rules do not apply to e-mails or texts from the patient. "The Security Rule … does not apply to the patient. A patient may send health information to you using email or texting that is not secure. That health information becomes protected by the HIPAA Rules when you receive it." (OCR Guide at p.31). Moreover,

> Patients may initiate communications with a provider using e-mail. If this situation occurs, the health care provider can assume (unless the patient has explicitly stated otherwise) that e-mail communications are acceptable to the individual. If the provider feels the patient may not be aware of the possible risks of using unencrypted e-mail, or has concerns about potential liability, the provider can alert the patient of those risks, and let the patient decide whether to continue e-mail communications.

(OCR FAQ, available at http://www.hhs.gov/ocr/privacy/hipaa/faq/health_information_technology/570.html). In the wake of the Omnibus Rule commentary quoted above, covered entities and business associates should warn patients of the security risks before responding via unsecure e-mail or text.

Texts and E-mails to Other Providers, Employees, or Third Parties. The HIPAA Privacy and Security Rules also apply to e-mails and texts to persons or entities other than patients. Unlike communications with patients, simply warning the third party that the communication may not be secure is not enough. Thus, although many providers do not think about it, they should generally not communicate e-PHI with their staff or other providers via unencrypted e-mail or text unless they have implemented appropriate safeguards consistent with Security Rule requirements. HHS recently posted the following FAQ for providers:

> Question: Can you use texting to communicate health information, even if it is to another provider or

professional?

Answer: It depends. Text messages are generally not secure because they lack encryption, and the sender does not know with certainty the message is received by the intended recipient. Also, the telecommunication vendor/wireless carrier may store the text messages. However, your organization may approve texting after performing a risk analysis or implementing a third-party messaging solution that incorporates measures to establish a secure communication platform that will allow texting on approved mobile devices.

(Available at https://www.healthit.gov/faq/can-you-use-texting-communicate-health-information-even-if-it-another-provider-or-professional). Suggestions for securing e-mail and text communications are discussed on HHS's HealthIT.gov website.

Conclusion. HIPAA allows covered entities and their business associates to communicate e-PHI with patients via e-mails and texts if either (1) the e-mails and texts are encrypted and/or are otherwise secure consistent with Security Rule standards; or (2) the covered entity or business associate first warns the patient that the communication is not secure and the patient elects to communicate via unsecure e-mail or text anyway. When it comes to communicating with non-patients, the covered entity or business associate must generally ensure that its e-mail or texts comply with relevant Privacy and Security Rule standards.

---

questions as to the application of the law to your activities, you should seek the advice of your legal counsel.