Caution: Sending Patient Information Via Text May Implicate HIPAA Penalties

by

Emily D. Armstrong

Are you or providers sending patient information via text? Are you or providers communicating about patients via text? If the answer to either of these questions is "yes," beware this could result in fines and legal violations.

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is a Federal law that addresses, in part, the security and privacy of health data. The law requires the Department of Health and Human Services ("HHS") to establish rules for the handling of protected health information ("PHI").[1]

One rule HHS implemented, the "Security Rule," establishes national standards to protect *electronic* PHI that is created, received, used, or maintained by a "covered entity."[2] A covered entity is generally a health care provider who electronically submits health care information in connection with certain transactions, a health plan, or a health care clearinghouse.[3]

The Security Rule requires a covered entity to implement three types of safeguards to ensure the confidentiality, integrity, and security of electronic PHI: (1) administrative (policies and procedures to protect PHI); (2) physical (physical measures to protect PHI); and (3) and technical (technology to protect PHI).

The technical safeguards require a covered entity to ensure that only authorized persons have to access to electronic PHI and to implement a mechanism to encrypt and decrypt electronic PHI. The technical safeguards also require a covered entity to track the persons with access to PHI, to establish mechanisms to ensure that PHI is not improperly altered or destroyed, and to implement measures to guard against unauthorized access to PHI.[4]

PHI in text messages is a form of electronic PHI. The Security Rule applies to any transmission of electronic PHI via text, and appropriate safeguards must be in place to ensure the privacy and security of PHI communicated by text.

Unfortunately, traditional mobile-to-mobile text messaging is non-secure because messages containing PHI can be read by anyone and forwarded to anyone. Text messages are also unencrypted and stay on senders' and receivers' phones.

The unsecure nature of text messaging caused the Joint Commission on Accreditation of Healthcare Organizations, a standard-setting healthcare organization, to disallow the use of traditional texts for transmitting PHI. Its FAQs state:

---

[1] 42 U.S.C. § 1320d *et seq.*

[2] The Security Rule is located at 45 C.F.R. Part 160 and Part 164, Subparts A and C.

[3] 45 C.F.R. § 160.103.

[4] 45 C.F.R. § 164.312.

> Is it acceptable for physicians and licensed independent practitioners (and other practitioners allowed to write orders) to text orders for patients to the hospital or other healthcare setting?
>
> No it is not acceptable for physicians or licensed independent practitioners to text orders for patients to the hospital or other healthcare setting. This method provides no ability to verify the identity of the person sending the text and there is no way to keep the original message as validation of what is entered into the medical record.[5]

Despite the Joint Commission's statement, if mobile devices contain the proper security measures required by HIPAA, theoretically providers can use those devices to communicate. HHS and the Office of the National Coordinator for Health Information Technology ("ONC") gathered tips to safeguard PHI when using mobile devices. They make the following suggestions about how to protect and secure information on mobile devices:

- Use a password or other user authentication.
- Install and enable encryption.
- Install and activate remote wiping and/or remote disabling.
- Disable and do not install or use file sharing applications.
- Install and enable a firewall.
- Install and enable security software.
- Keep your security software up to date.
- Research mobile applications (apps) before downloading.
- Maintain physical control of the mobile device.
- Use adequate security to send or receive health information over public Wi-Fi networks.
- Delete all stored health information before discarding or reusing the mobile device.[6]

HHS and ONC also recommended five steps for covered entities to follow when managing PHI transmitted via mobile devices:

1. Decide whether mobile devices will be used to access, receive, transmit, or store patients' health information or used as part of your organization's internal networks or systems (e.g., your EHR system).

2. Consider how mobile devices affect the risks (threats and vulnerabilities) to the health information your organization holds.

---

[5] http://www.jointcommission.org/standards_information/jcfaqdetails.aspx?StandardsFaqId=401&ProgramId=47

[6] http://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device

3. Identify your organization's mobile device risk management strategy, including privacy and security safeguards.

4. Develop, document, and implement the organization's mobile device policies and procedures to safeguard health information.

5. Conduct mobile device privacy and security awareness and training for providers and professionals.[7]

If these precautions are implemented and followed, mobile-to-mobile data exchange could be secure. However, it should be noted that these tips are not included in the law and must be analyzed in tandem with HIPAA regulations and guidance.[8]

Some mobile carriers and providers are now claiming to offer secure, fully encrypted, text messaging. Covered entities looking to use such technology should consult with their attorneys and compliance officers, however, to ensure that the technology complies with HIPAA. If PHI is sent via non-secure text messages, each text is a HIPAA violation and can result in a hefty fine.

Given the potential fines and the Joint Commission's and other organizations' stark warnings against using text messages, providers should prohibit the use of text messaging for transmitting patient information until their technology and applications have been analyzed and vetted through proper compliance channels. To accomplish this, we recommend you (1) immediately instruct all providers to cease this practice, (2) investigate and assess the electronic communications practices providers have been using, and (3) then consult with appropriate persons on implementing a HIPAA compliant electronic communication method.

[7] http://www.healthit.gov/providers-professionals/five-steps-organizations-can-take-manage-mobile-devices-used-health-care-pro

[8] The HIPAA regulations regarding the safeguards necessary to protect electronic PHI are summarized above. However, this should not be considered an exhaustive list of HIPAA requirements and providers should consult with their attorneys and compliance officers regarding same.