HARWOOD LLOYD

The Transmission of HIPAA Regulated Protected Health Information Between a HIPAA Covered Entity and a Patient via E-Mail – Must it be Encrypted?

By David Meinhard, Esq.
Harwood Lloyd, LLC
March 2017

QUESTION

A physician asked the following: If a patient wants to send a physician or other HIPAA Covered Entity (CE) electronic copies of her medical records from a prior physician, and is insisting that she send the medical records via unencrypted e-mail, should the CE agree to the patient's request? If she sends her medical records from another physician via unencrypted e-mail, will the CE's acceptance and use of those records be in violation of the HIPAA Privacy and Security regulations? What about if the CE then respond to her e-mails via non-encrypted e-mail, where Protected Health Information (PHI) is included - will that violate HIPAA?

ANSWER

- Encryption is an "addressable standard" under the HIPAA Security Rule[i], such that a HIPAA Covered Entity must evaluate its operations to determine whether it deems it necessary to encrypt PHI made transmitted via e-mail. The need to implement addressable standards vary based on the size, complexity and capabilities of the CE, with smaller CE's (such as a small physician practice) having a lesser burden than a large CE (such as a hospital).[ii]

- It is generally recommended that when e-mailing PHI it should be encrypted, using an end-to-end encryption method. If a CE does not have an encrypted e-mail solution to use, it is prudent not to send PHI via e-mail, however, to address occasional transmissions between a CE and patient, where the patient is insistent on sending PHI via unencrypted e-mail, it would be acceptable to do so, provided the CE has documentation that it warned the patient of the risk of a 3rd party accessing the PHI sent in this manner. The documentation should be clear, and the CE will want to be able to have evidence that the document was signed by the patient or seen by the patient. At a minimum the CE may want an e-mail from the patient which indicates that she was advised of the risk associated with non-encrypted e-mail, and that the patient chose to accept that risk.[iii]

- Patients have a right to access PHI which is deemed to be part of a Designated Record Set[iv], so to the extent the CE chooses not to electronically transmit the PHI via e-mail it should advise the patient of other ways of transmitting the PHI to or from her, which could include through regular mail.[v]

Whenever communicating with patients a healthcare provider should also be mindful of complying with any other ethical or legal duties under state or other laws, which could be more restrictive than HIPAA, applicable to its practice regarding how and what the provider communicates to its patients.

David Meinhard is a transactional and regulatory lawyer, with a practice concentration in health care and privacy law, at Harwood Lloyd, LLC, located in Hackensack, NJ.

This article is offered for informational purposes and does not constitute a legal solicitation or the provision of legal advice. The information above should not be used as a substitute for obtaining legal advice from a qualified and licensed attorney.

© 2017 David Meinhard. All rights reserved.

[i] **45 CFR 164.312 Technical Safeguards**
(a)(2)(iv) *Encryption and decryption (Addressable).* Implement a mechanism to encrypt and decrypt electronic protected health information.

[ii] **45 CFR 164.306 Security Standards: General Rules**
In deciding which security measures to use, a covered entity or business associate must take into account the following factors: (i) The size, complexity, and capabilities of the covered entity or business associate. (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures. (iv) The probability and criticality of potential risks to electronic protected health information.

[iii] **From the January,25, 2013 HIPAA Final Rule, Fed Reg. (Vol 78, No.17) at page 5634**

Comment:
Several commenters specifically commented on the option to provide electronic protected health information via unencrypted email. Covered entities requested clarification that they are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email. Some felt that the "duty to warn" individuals of risks associated with unencrypted email would be unduly burdensome on covered entities. Covered entities also requested clarification that they would not be responsible for breach notification in the event that unauthorized access of protected health information occurred as a result of sending an unencrypted email based on an individual's request. Finally, one commenter emphasized the importance that individuals are allowed to decide if they want to receive unencrypted emails.

Response: We clarify that 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. Further, covered entities are not responsible for safeguarding information once delivered to the individual.

[iv] **45 CFR 164.501**

Designated record set means:

(1) A group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;

(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

[v] **45 CFR 164.524 Access of individuals to protected health information.**

(a)*Standard: Access to protected health information* -

(1)*Right of access.* Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set….