



C. Scott Litch

Chief Operating Officer and General Counsel

Litch's Law Log

Sending Protected Health Information via Unencrypted E-mail

This column in the March 2016 *PDT* addressed legalities of calling, texting, and e-mailing parents/guardians. It was noted that HIPAA does not require encryption of e-mails containing protected health information (PHI) in all circumstances. However, if you are communicating with a parent/guardian with an unencrypted e-mail, you can protect against legal liability by notifying the parent/guardian of the risks of third party disclosure. If they still prefer to receive PHI via an unencrypted e-mail, they have that right.

D-HHS recently released an updated set of HIPAA FAQs, and two of them go into greater detail on this point.¹ These are reproduced below for your convenience. I have highlighted key text. **The bottom line is that if you follow these procedures you can e-mail PHI to parents/guardians via unencrypted e-mail.**

“Do individuals have the right under HIPAA to have copies of their PHI transferred or transmitted to them in the manner they request, even if the requested mode of transfer or transmission is unsecure?”

Yes, as long as the PHI is “readily producible” in the manner requested, based on the capabilities of the covered entity and transmission or transfer in such a manner would not present an unacceptable level of security risk to the PHI on the covered entity’s systems, such as risks that may be presented by connecting an outside system, application, or device directly to a covered entity’s systems (as opposed to security risks to PHI once it has left the systems). For example, individuals generally have a right to receive copies of their PHI by mail or e-mail, if they request. It is expected that all covered entities have the capability to transmit PHI by mail or e-mail and transmitting PHI in such a manner does not present unacceptable security risks to the systems of covered entities, even though there may be security risks to the PHI once it has left the systems. Thus, a covered entity may not require that an individual travel to the covered entity’s physical location to pick up a copy of her PHI if the individual requests the copy be mailed or e-mailed. In the limited case where a covered entity is unable to e-mail the PHI as requested, such as in the case where diagnostic images are requested and e-mail cannot accommodate the file size of the images, the covered entity should offer the individual alternative means of receiving the PHI, such as on portable media that can be mailed to the individual.

Further, while covered entities are required by the Privacy and Security Rules to implement reasonable safeguards to protect PHI while in transit, individuals have a right to receive a copy of their PHI by unencrypted e-mail if the individual requests access in this manner. **In such cases, the covered entity must provide a brief warning to the individual that there is some level of risk that the individual’s PHI could be read or otherwise accessed by a third party while in transit, and confirm that the individual still wants to receive her PHI by unencrypted e-mail.** If the individual says yes, the covered entity must comply with the request. We note that providers using the 2015 edition of Certified EHR Technology will have the capability to send unencrypted e-mail transmissions directly from that technology.

Whether an individual has a right to receive a copy of her PHI through other unsecure modes of transmission or transfer (assuming the individual requests the mode and accepts the risk) depends on the extent to which the mode of transmission or transfer is within the capabilities of the covered entity and the mode would not present an unacceptable level of risk to the security of the PHI on the covered entity’s systems (as explained above), based on the covered entity’s Security Rule risk analysis. For example, a covered entity’s risk analysis may provide that connecting an outside (foreign) device, such as a USB drive, directly to the entity’s systems presents an unacceptable level of risk to the PHI on the systems. In this case, the covered entity is not required to agree to an individual’s request to transfer the PHI in this manner, but the entity must offer some other means of providing electronic access to the PHI.

Note that while an individual can receive copies of her PHI by unsecure methods if that is her preference, as described in more detail above, a covered entity is not permitted **to require** an individual to accept unsecure methods of transmission in order to receive copies of her health information.

Is a covered entity responsible if it complies with an individual's access request to receive PHI in an unsecure manner (e.g., unencrypted e-mail) and the information is intercepted while in transit?

No. While covered entities are responsible for adopting reasonable safeguards in implementing the individual's request (e.g., correctly entering the e-mail address), covered entities are not responsible for a disclosure of PHI **while in transmission** to the individual based on the individual's access request to receive the PHI in an unsecure manner (assuming the individual was warned of and accepted the risks associated with the unsecure transmission). This includes breach notification obligations and liability for disclosures that occur in transit. Further, covered entities are not responsible for safeguarding the information once delivered to the individual. Covered entities are responsible for breach notification for unsecured transmissions and may be liable for impermissible disclosures of PHI that occur in all contexts except when fulfilling an individual's right of access under 45 CFR 164.524 to receive his or her PHI or direct the PHI to a third party in an unsecure manner."

For further information contact Chief Operating Officer and General Counsel C. Scott Litch at 312-337-2169 ext. 29 or slitch@aapd.org.

This column presents a general informational overview of legal issues. It is intended as general guidance rather than legal advice. It is not a substitute for consulting with your own attorney concerning specific circumstances in your dental practice. Mr. Litch does not provide legal representation to individual AAPD members.

¹ <http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html>

Tastes better. Won't clump. Costs less.

Introducing wonderfl™
Better flavors, better formula
Chocolate and Spearmint



 **wonderfl™**
FLUORIDE VARNISH

We only sell direct.
We save you money.
888.667.9475