Health Information Compliance Alert

Security: Tales From Encryption: Don't Turn E-mail Security Into A Horror Story

New Solutions To Secure E-mail Transmissions

If you haven't evaluated both data in transfer and data at rest, the next time you click "send" could result in a HIPAA violation.

HIPAA's final security rule doesn't mandate that you encrypt all of your e-mail transmissions, but it does require you to examine how all your data is transferred communicatively. When you begin to evaluate how you transmit electronic protected health information, you'll need to consider two important topics from the get-go: integrity controls and encryption.

Integrity control really just means proper access controls and login procedures, password restriction and other user authorizations - the basics of your e-mail policies. Integrity control also represents mainly a policy approach to e-mail security; that is, making sure your staff members know what e-mail procedures are permitted within your organization. It's important to keep in mind that your organization may not need to encrypt e-mail.

For example, small covered entities like a small physician office that's full of familiar faces and equipped with a straightforward network probably wouldn't require encryption, while a 200-bed hospital with dozens of physicians might need greater e-mail security.

Different Orgs, Different Needs

Obviously, not all organizations will have the same security needs: Academic medical centers are completely different animals compared to small medical centers. Take the **University of Florida**, for example. UF's Privacy Office recently had to redefine its e-mail policy. The university permits certain provider-to-provider (or provider-to-staff) e-mails, but only for limited purposes (e.g., prescription refills, consultations, referrals, and billing inquiries), and providers must use the minimum necessary approach when including PHI in e-mail messages. For provider-to-patient e-mail messaging, UF's process remains nearly the same. After giving the patient cautionary information about e-mail security, the provider must obtain a signed patient authorization to permit e-mail communications. The university has even created a HIPAA-compliant e-mail authorization form available for the patient's signature (see sample document).

"The big thing that everyone needs to understand about the security rule is that they need to evaluate all of their information, both info that's being transferred on a communications basis, but also info that they have at rest."

- Jim Sheldon-Dean, consultant

"We have a decentralized server environment here at the university, so what we've elected to do is set boundaries on what we can do for routine practice and then what we can do if we go over the Internet," explains **Susan Blair**, privacy officer with the Office of Vice-President for Health Affairs at the University of Florida. "Our policy allows four specific purposes for e-mail: prescription refills, consultation, referral, and billing - [and e-mail may be used] only for those purposes."

Blair says UF also conducts random audits to ensure people are in compliance. "They're random, they're ongoing, and if we see some unusual patterns, we act immediately on that," she tells **Eli**.

CPT® 2023 American Medical Association. All rights reserved.

But the policies developed by Blair and the university won't necessarily work for everyone. Smaller medical offices, like **Casa Grande Medical Center** (CGMC) in Casa Grande, AZ have developed their own e-mail policies, but the center's privacy officer, **Becky Buegel**, says, "everybody's swearing up and down they're not using e-mail to send any PHI out of the building." And that pledge may be true, because CGMC only staffs a few doctors.

Buegel says PHI might be sent by e-mail internally, but it's not encrypted for such use. "I'm comfortable with that because of the size of our organization and our lack of sophistication when it comes to electronic media."

Encryption Not Always Vital

Whether you eventually encrypt your e-mail transmissions depends on a number of factors, and you should consider at least five variables, according to **Jim Sheldon-Dean**, director of HIPAA compliance with **Lewis Creek Systems** in Charlotte, VT. Ask yourself these questions as you assess your security needs:

#1 How critical is the information being transmitted?;

#2 What is the completeness of the information? That is, is this a complete medical record or is this just a snippet of information?;

#3 How many individuals might be represented in the information? In other words, information about one person would have a different weight than information about a group of people;

#4 What is the level of the network's security? That's where you start to consider whether it's a local network or the Internet, says Sheldon-Dean; and

#5 What are your organizational factors? This includes how big your organization is and what are the capabilities of your organization. For example, hospitals should be able to handle a lot more technical tasks more easily than a one-physician doctor's office (for more examples, see article "Not Sure Whether Encryption's For You? 4 Examples Will Help You Decide").

If you're not sure how to answer these questions, it's likely you'll need to encrypt. But whatever you decide to do, don't fret about not being particularly tech-savvy - encryption, if you decide to go that route, isn't really that complicated. You probably have a vendor that you're used to dealing with who should be able to steer you in the right direction for not a whole lot of money, or your own IT people may have a recommendation, says Sheldon-Dean.

CPT® 2023 American Medical Association. All rights reserved.