Think Your Practice is HIPAA Compliant? Think Again.

June 08, 2015 | HIPAA [1], Audits [2], EHR [3], Operations [4], Technology [5]
By Aubrey Westgate [6]

Nine HIPAA missteps that experts say medical practices make every day.
Source: Physicians Practice

You may think you know HIPAA inside and out, but experts say many practices and physicians are making mistakes regarding protected health information (PHI) that could get them into big trouble with the law. Here are nine of the most common compliance missteps they say practices and physicians are making.

1. **TEXTING UNENCRYPTED PHI**
For most physicians, texting is an easy, convenient, and efficient way to communicate with patients and colleagues. But if a text contains unencrypted PHI, that could raise serious HIPAA problems. "One of the big things people are doing these days is texting PHI, and people seem to be ignoring the fact that text messages can be read by anyone, they can be forwarded to anyone, [and] they're not encrypted in any fashion when they reside on a telecommunications provider's server," says Jim Hook, director of consulting services at healthcare consulting firm The Fox Group, LLC. "People really need to understand that [short message service (SMS)] text messaging is inherently nonsecure, and it's noncompliant with HIPAA."

That's not to say that texting PHI is never appropriate, it just means that physicians must find a way to do so securely. While the privacy and security rules don't provide explicit text messaging guidelines, they do state that covered entities must have "reasonable and appropriate safeguards to protect the confidentiality, availability, and integrity of protected health information," says Michelle Caswell, senior director, legal and compliance, at healthcare risk-management consulting firm Clearwater Compliance, LLC. As a result, Caswell, who formerly worked for HHS' Office for Civil Rights, says physicians must consider, "What would I put on my [smart] phone to reasonably and appropriately safeguard that information?" Most likely, the answer will be a secure messaging service with encryption, she says, adding that many inexpensive solutions are available to providers.

2. **E-MAILING UNENCRYPTED PHI**
Similar to text messaging, many physicians are e-mailing unencrypted PHI to patients and colleagues. As Robert Tennant, senior policy adviser of government affairs for the Medical Group Management Association says, e-mailing is becoming ubiquitous in our society, and healthcare is no exception.

If your providers are e-mailing PHI, consider implementing a secure e-mail application; for instance, one that recognizes when content included in the e-mail contains sensitive information and therefore automatically encrypts the e-mail. Your practice could use the application to specify certain circumstances in which e-mails should be encrypted; such as the inclusion of social security numbers or credit card numbers. The application would then filter e-mails for that specified content, and when it finds that content, encrypt those e-mails automatically, says Caswell.

Another option is to use a secure e-mail application to set up filters to automatically encrypt e-mails sent with attachments, or encrypt e-mails when senders include a word like "sensitive" or "encrypt" in the subject line, she says. An added benefit of encrypting e-mail is if a potential breach occurs, like the theft of a laptop containing e-mails with PHI, that is not considered a reportable breach if the e-mails stored on the laptop are encrypted, says Tennant. "You don't need to go through all of the rigmarole in terms of reporting the breach to the affected individual, and ultimately, to the government," he says. "So it's sort of a get out of jail free card in that sense."

If your practice would rather prohibit the use of e-mail altogether, a great alternative might be a patient portal that enables secure messaging.

Finally, if patients insist on having PHI e-mailed to them despite the risks, get their permission in writing for you to send and receive their e-mails, says Tennant.

* For more guidance on what constitutes a reportable breach, visit [bit.ly/reportable-breach].

3. **Failing to Conduct a Risk Analysis**
If your practice has not conducted a security risk analysis — and about 31 percent of you have not,
according to our 2014 Technology Survey, Sponsored by Kareo — it is violating HIPAA. The security rule requires any covered entity creating or storing PHI electronically to perform one. Essentially, this means practices must go through a series of steps to assess potential risks and vulnerabilities to the confidentiality, integrity, and availability of their electronic protected health information (ePHI).

Though the security risk analysis requirement has been in place since the security rule was formally adopted in 2003, it’s been pretty widely ignored by practices, says Hook. Part of the reason, he says, is lack of enforcement of the requirement until recently. Since conducting a security risk analysis is now an attestation requirement in the EHR incentive program, auditors are increasingly noting whether practices are in compliance.

4. FAILING TO UPDATE THE NPP

If your practice has not updated its Notice of Privacy Practices (NPP) recently, it could be violating HIPAA. The HIPAA Omnibus Rule requires practices to update these policies and take additional steps to ensure patients are aware of them, says Tennant. Some of the required updates to the NPP include:

• Information regarding uses and disclosures that require authorization;
• Information about an individual's right to restrict certain disclosures of PHI to a health plan; and
• Information regarding an affected individual's right to be notified following a privacy or security breach.

In addition to updating the NPP, a practice must post it prominently in its facility and on the website, and have new patients sign it and offer a copy to them, says Tennant. "I'd say of every 10 practices, hospitals, dental offices I go into, nine of them don't have their privacy notice in the waiting room," he says.

• For more guidance on NPP updates, visit bit.ly/npp-update.
• For a sample NPP, visit bit.ly/npp-sample.

5. IGNORING RECORD AMMENDMENT REQUESTS

Don't hesitate to take action when patients request an amendment to information in their medical records, cautions Cindy Winn, deputy director of consulting services at The Fox Group, LLC. Under the HIPAA Privacy Rule, patients have the right to request a change to their records, and providers must act on those requests within 60 days, she says.

If you disagree with a patient's requested change, you must explain, in writing, why you are not making the requested change, says Hook. Then, share that reasoning with the patient and store a copy of it in the patient's medical record, as well as a copy of the patient's written request for the amendment.

• For more guidance, visit bit.ly/patient-change-requests.

6. NOT PROVIDING ENOUGH TRAINING

The privacy and security rules require formal HIPAA education and training of staff. Though the rules don't provide detailed guidance regarding what training is required, Hook recommends training all the members of your workforce on policies and procedures that address privacy and security at the time of hire, and at least annually thereafter.

The HIPAA Security Rule also requires practices to provide "periodic security reminders" to staff, says Caswell, adding that many practices are unaware of this. Actions that might satisfy this requirement include sending e-mails to staff when privacy and security issues come up in the news, such as information about a recent malware outbreak; or inserting a regular "security awareness" column in staff e-newsletters.

Finally, be sure to document any HIPAA training provided to staff.

7. OVERCHARGING FOR RECORD COPIES

With few exceptions, the privacy rule requires practices to provide patients with copies of their medical records when requested. It also requires you to provide access to the record in the form requested by the individual, if it is readily producible in that manner.

While practices can charge for copies of records, some practices may be getting into trouble due to the fee they are charging, says Tennant. "HIPAA is pretty clear that you can only charge a cost-based fee and most of those are set by the state, so most states have [limits such as] 50 cents a page up to maybe $1 a page ... but you can't charge a $50 handling fee or processing fee; at least it's highly discouraged," says Tennant.

To ensure you are following the appropriate guidelines when dealing with record copy requests, review your state's regulations and consult an attorney. Also, keep in mind that though the privacy rule requires practices to provide copies within 30 days of the request, some states require even shorter timeframes.
8. BEING TOO OPEN WITH ACCESS

If your practice does not have security controls in place regarding who can access what medical records and in what situations, it's setting itself up for a HIPAA violation. The privacy rule requires that only those who have a valid reason to access a patient's record — treatment purposes, payment purposes, or healthcare operations — should do so, says Caswell. "If none of those things exist, then a person shouldn't [access] an individual's chart."

Caswell says practices need to take steps to ensure that staff members do not participate in "record snooping" — inappropriately accessing a neighbor's record, a family member's record, or even their own record.

She recommends practices take the following precautions:

- Train staff on appropriate record access;
- Implement policies related to appropriate record access; and
- Run EHR audits regularly to determine whether inappropriate access is occurring.

9. RELEASING TOO MUCH INFORMATION

Similar to providing too much access to staff, some practices provide too much access to outside entities, says Caswell. For instance, they release too much PHI when responding to requests such as subpoenas for medical records, requests for immunization information from schools, or requests for information from a payer.

"If there's, say, for instance, litigation going on and an attorney says, 'I need the record from December 2012 to February 2014,' it is your responsibility to only send that amount of information and not send anything else, so sort of applying what's called the minimum necessary standard," says Caswell. "When you receive outside requests for PHI, pay close attention to the dates for which information is requested, as well as the specific information requested."

Aubrey Westgate is senior editor for Physicians Practice. She can be reached at aubrey.westgate@ubm.com.

This article originally appeared in the June 2015 issue of Physicians Practice.