

Your Podiatry Practice and HIPAA: Twelve Scenarios

It's important to protect PHI.

BY LAWRENCE F. KOBAK, DPM, JD

Many podiatrists do not understand the HIPAA law. The key is understanding what is Protected Health Information (PHI). PHI is any payment or medical record that makes the person in question identifiable. Any identifying data, name, or email address qualifies. Your patient may request a copy of their records, paper or EMR format. It generally must be provided within 30 days. A patient's PHI may be shared with other currently treating healthcare providers.

Scenario 1

A patient is in a treatment room. In that room is what appears to be a clothing closet with unlocked sliding doors. Stacked on the floor are piles of "old" paper patient records. Patient paper charts may not be kept unlocked in treatment room closets! Additionally, unguarded or unlocked vertical files behind the front desk are also not allowed. Patient files left on desks waiting to be filled out are also a HIPAA violation when left unguarded. Common sense and the law dictate that accessible PHI is not permitted in your office.

Scenario 2

A computer's monitor is left on with the last patient's records on

the screen. It is the monitor next to the podiatrist's chair. It is easily visible when the patient walks in the treatment room. EMR patient

password-protected by the healthcare provider. PHI should only be accessed on a need-to-know basis. A healthcare provider should not share

Your staff must be trained in the HIPAA law and what is PHI and how to keep it confidential.

records should not be left on a monitor in a treatment room for anyone to see. The screen should be closed after each healthcare provider's use or at least on the records of the patient entering the room. The computer access should be individually

their password with another provider in order to facilitate access to the medical records.

Scenario 3

Your practice uses a blood lab. PHI along with the orders for that patient go to the lab. You most likely use third party vendors that require you to use patient names for various reasons: lab tests, radiology, orthotics, billing.

You MUST have a signed Business Associate Agreement with each of these parties as they are handling PHI. They must treat it in the same way you do. Joe Jones, who works at the lab, cannot share with Mary Smith that a patient had a toxicology test, a culture and sensitivity, or any other PHI.

Scenario 4

Your podiatric assistant notes that your patient history on Ms. Jones, her friend and neighbor, includes an abortion and a venereal disease. She shares this

Continued on page 66



HIPAA (from page 65)

spicy tidbit with her sister as soon as she gets home. This is a blatant HIPAA violation and could result in a significant fine. Your staff must be trained in the HIPAA law and what is PHI and how to keep it confidential. As an aside, unless the podiatric assistant had a good reason involving some aspect of patient care to read the patient's medical history, that too is not allowed under the HIPAA laws.

Scenario 5

You have a very unusual case. You decide to "publish it" on the Internet. Something in your post makes the identity of your patient clear. Even though you may have the best intentions to enlighten the podiatric community, that is a HIPAA violation without the expressed consent of the patient; make sure any photos of feet or x-rays have no showing identifiable information as to who the patient is.

Scenario 6

The details of HIPAA are important, and this column can easily become a chapter or book in and of itself. A good rule of thumb is disclosing nothing that you would not want disclosed about yourself. Make

via a secure method. Additionally, make sure that your transcription service observes HIPAA and have them sign a Business Associate Agreement.

ric patients. The father was from an affair. This was texted, by mistake, to the patient's mother. The text had NOT been sent to anyone

**The best practice is to encrypt your files.
Most modern EMR software makes that possible.**

Most healthcare attorneys can help you with this.

Scenario 8

You are travelling from one office to another with your computer. It contains patient records. You inadvertently leave it in the car, and it is stolen. Your car was locked. You neglected to have a lock on the computer or even place a password on the files let alone encrypt the files. You have breached HIPAA. The best practice is to encrypt your files. Most modern EMR software makes that possible. Secure cloud computing would help obviate this entire concern as the files would not be on your computer hard drive; they would be stored in the cloud.

Scenario 9

You have your laptop in the Uber and you mistakenly leave it there.

but the minor patient's mother. We successfully argued the PHI was not disclosed to anyone else. From the text, it was NOT clear who the mother was. However, the mother reported the physician to the medical board. As the identity was not revealed, the doctor got off with a warning. My warning is not to do that—ever! Would you want your healthcare provider spreading stories like that? This occurred in a relatively small town. It is hard to divorce one's healthcare practice from one's social life. The safe way is to KEEP YOUR MOUTH SHUT and your thumbs away from texting anything you do not want the world to know.

Scenario 11

The podiatrist left a message on the cell phone number given by the patient on the intake. The patient was explicit in stating that any message can be left on that line. The podiatrist left a message with that number as to the results of the patient's blood test. It turned out that the bunion surgery had to be postponed due to a positive pre-op pregnancy test. Her husband (not the father) picked up his wife's phone messages and got the shocking news. The podiatrist did not violate HIPAA. He was acting with the consent of the patient. The best practice is to obtain that consent to use that number in writing. Have the patient sign off on that part of the intake sheet. Of course, it is better not to leave substantive messages concerning a patient's medical status on an answering machine.

Scenario 12

The podiatrist had just finished his successful testimony as an expert witness at trial. His testimony

Continued on page 68

A good rule of thumb is disclosing nothing that you would not want disclosed about yourself.

sure your staff knows that too. They will need training. Until next time.

Scenario 7

You have just taken your patient's vital signs and examined her pulses and deep tendon reflexes. You decide to text that information to your scribe service in a remote location to enter it into the patient chart, either through a cloud EMR or otherwise. This potentially places this patient's PHI at jeopardy. It could be intercepted by the wrong people. Enter this information directly into your local terminal. If you are using a remote transcription service, make sure you are sending them your data

You cannot find it. However, your files containing PHI were securely backed-up and encrypted with FIPS 140-2 encryption (Federal Government security standard). You should be fine! Same scenario, but not encrypted... you would have to notify every patient who had PHI on your computer that their PHI might have been compromised and go through a formal reporting protocol that is beyond the scope of this article. There may be heavy fines involved.

Scenario 10

This really happened! A pediatrician sent a message regarding the "parentage" of one his pediat-

HIPAA (from page 66)

deftly demonstrated that the foot and ankle surgeon performed the surgery at or above the standard of care. The untoward result had noth-

dly careless with someone else's medical records. As the defendant's expert witness, he had a right to review and have a copy of the medical records. After trial, he should have destroyed them or returned

Use common sense when it comes to HIPAA. Would you want your PHI dealt with in a careless or haphazard way? I doubt it. Why not afford your patients the same protection? Treating your patients with respect will be repaid tenfold. **PM**

Use common sense when it comes to HIPAA. Would you want your PHI dealt with in a careless or haphazard way?

ing to do with the doc's negligence. On the way out of the courtroom, he dumps the plaintiff's medical records in the trash. This had been a high-profile trial. An alert reporter retrieved the medical records from the trash and included some interesting "facts" in her article in the morning newspaper. This is a HIPAA violation.

The podiatric expert was un-

them to the defendant's attorney. The medical records showed in the medical history that the plaintiff had an abortion 20 years prior, totally irrelevant to the issues of the trial. While the plaintiff put her bunionectomy and her relevant medical condition at issue, she did not sign on to having her medical records turning up in the morning newspaper.



Dr. Kobak is Senior Counsel in Frier Levitt's Healthcare Department in the Uniondale, New York. Larry has extensive experience representing physicians in connection with licensure issues, as well as successfully defending physicians before Medical Boards, OPMC, OPD investigations, as well as Medicare Fraud, Fraud & Abuse, Hospital Actions, RAC Audits, Medicare Audits, OIG Fraud, Health Care Fraud, Medical Audits, and Health Plan Billing Audits. As a licensed podiatrist prior to becoming an attorney, he served as the international president of the Academy of Ambulatory Foot and Ankle Surgery.
