Codify
BY AAPC

Health Information Compliance Alert

Patient Privacy: Avoid These Cell Phone HIPAA Land Mines

Contacting on-call physicians via text or mobile phone? Make sure those communications are HIPAA-compliant.

Mobile phones may go hand-in-hand with busy physicians who must be reachable at all times, but when it comes to HIPAA safety, these ubiquitous devices can be a thorn in your side. Make sure you are using your cell phones in a HIPAA-appropriate way with these quick tips.

Ensure the Safety of Emails and Texts

Scenario: Your on-call physician asks you to contact him if any patients phone in. When you call his cell phone, he texts back saying that he can't talk but he also requests details about the sick patient's condition via text. Can you text him back with a patient's protected health information (PHI), or is that forbidden?

The facts: Technically, texting the information to the physician is not illegal under HIPAA, but it might not be allowed under your state law -- and could put your practice at risk either way.

"There are at least two sets of laws to consider here -- HIPAA and state law," says **Stephen W. Bernstein, Esq.,** international head of the Health Industry Practice Group with McDermott Will & Emery, LLP in Boston. "If the state law is more protective, it wins." Therefore, your first order of business is to determine whether your state prohibits the texting of PHI.

If your state law doesn't address the issue, you should work under HIPAA regulations, which require medical practices to evaluate whether an action should be taken to secure various types of technology and the information contained in it. "From a HIPAA security standpoint, it's better not to send emails and texts, but between the two, emails are safer than texts, and when possible, emails should be encrypted," Bernstein says.

Why texts are risky: "Generally speaking, text messages are not encrypted," says **Patricia A. Markus, Esq.,** a partner with the Health Care Team of Smith Moore Leatherwood LLP in Raleigh, N.C. "Sometimes, a hospital or medical practice will purchase and provide cell phones to its employees, including employed physicians, and the hospital or practice also will apply encryption software or applications to the cell phones. However, this is the exception, not the rule," she notes.

Without encryption, the physician who texts information about patients, including patient names and conditions, is taking a big risk, Markus says. "If the text message containing PHI is sent to the wrong number and received by a person not authorized to know that information, then a breach of that patient's PHI has occurred, and the physician will have to evaluate whether to provide notification of the breach to the patient and the Secretary of HHS pursuant to the HITECH Act's breach notification requirements."

In addition, "text messages most likely will be stored on the cell phone's computer or SIM card, so if the physician loses his or her cell phone, a person finding the phone may be able to access text messages containing PHI," she notes. "A friend or relative of the physician who uses the physician's cell phone also could discover this information."

Other than encryption, ways to limit the likelihood of a HIPAA violation when texting PHI include not identifying patients by name or social security number, but instead using medical record numbers. "This tactic isn't foolproof, however, as other information included in a description of the patient's condition might be used by an unauthorized person to identify the patient," Markus says. "Password protecting cell phones always is a good idea, as doing this can minimize the likelihood that an unauthorized person using a physician's lost or stolen phone would be able to access information stored on the phone unless that person knows or guesses the password."

What the law says: The HIPAA Security Rule requires physicians and hospitals to protect against reasonably anticipated threats or risks to the security or integrity of PHI. "Since mobile devices are lost or stolen every day and unauthorized access to information contained on such devices occurs regularly, the Office for Civil Rights likely would determine that texting PHI on unencrypted cell phones does not comply with the HIPAA Security Rule's requirements," Markus says. Rather than saving a minute or two by texting on an unencrypted device, hospitals and physicians "should strongly consider either encrypting cell phones or using another, safer method (secure e-mail, telephone calls) to transmit updates on patients," she adds.

A Picture May Be Worth Thousands of Dollars

Most cell phones in use today feature digital cameras, making it simple to take photographs with mobile devices. But taking pictures that might compromise patient safety could land you in hot water. In 2009, two nurses photographed a patient who was getting an x-ray at a medical center where they worked, and one of them posted the photo on the Internet. The nurses were subsequently fired for violating patient privacy.

Although you may not think your practice uses mobile phone cameras often, consider office birthdays or other events when you shoot photographs of staff members, and think about the likelihood that a patient might show up in the background. Sharing that photograph could mean compromising a patient's privacy.

"Patients in a doctor's office have some expectation of privacy, and certainly privacy from a physician and her own staff, so the doctor's staff shouldn't be snapping pictures with patients around," Bernstein says. "Although it's probably overkill to have a big sign that says 'No Photos Allowed,' staff members should be trained and you should maintain an internal policy on the use of cameras in a patient setting."

If your practice photographs patients for medical records and identification purposes, you should maintain office policies on how those photos will be utilized. "Generally speaking, photos should not be taken of any patients without first obtaining the patient's written consent and providing notice to the patient about the specific uses which will be made of the photos," Markus says.

In addition, make sure your office invests in a camera that will stay on-site permanently. "It generally is not a good idea to permit the use of personally-owned camera phones for work-related photos," Markus says. "Instead, facility-owned cameras should be used. That way, the provider can better assure that the images are appropriately stored, used only for permitted purposes, and not forwarded to unauthorized third parties or posted on social media websites. Training on the facility's camera phone policies is critical to assure that all employees and volunteers understand and abide by the rules."