Ignorance is no defense

By **MICHAEL McBRIDE**, *Technology Editor*

Alexandra Thran, MD, a practicing emergency department physician, was fired by a Rhode Island hospital, and subsequently was officially reprimanded and fined, for posting electronic protected health information (PHI) online. You might remember the case. It took place in 2010 and was covered nationally in the media. It was the first such incident in Rhode Island of a caregiver being fired or severely chastised for violating a healthcare organization's PHI privacy policy. Nationwide, however, it would not be the last.

A year earlier, the *Journal of the American Medical Association* published an article, "Online posting of unprofessional content by medical students," that revealed the results of an anonymous electronic survey sent to the deans of 130 medical schools. Of those who responded to the survey:

- 60% (47 of 78 respondents) reported incidents of students posting unprofessional content online.
- 52% (22 of 42) reported student use of profanity.
- 48% (19 of 40) reported use of "frankly discriminatory" language.
- 39% (17 of 44) reported the depiction of intoxication.
- 38% (16 or 42) reported the posting of sexually suggestive material.
- 13% (6 of 46) reported violations of patient confidentiality.

Of those schools who imposed punishment:

- 67% (30) gave informal warnings.
- 7% (3) dismissed students.

It's imperative that you understand the laws concerning patient privacy as well as the PHI policies of any hospitals at which you practice medicine.

SIDESTEPPING QUICKSAND

I recently read an article posted online by a physician sharing several ways he uses a smartphone in his practice. For instance, he takes snapshots of his patients' records so he can complete his notes away from the practice's physical location. Nowhere in the 4-page article did he mention the Health Insurance Portability and Accountability Act (HIPAA).

The U.S. Department of Health and Human Services (HHS) expects covered entities—physicians and hospitals—to implement policies governing the transmission and storage of PHI on mobile devices. Among other things:

- Devices must be password-protected.
- The PHI data on the devices must be encrypted.

Those two requirements are easy to implement and represent only a fraction of the HHS requirements, yet many portable-device users believe that using passwords or encrypting data are inconvenient precautions to take. Therefore, most of the PHI being carted around by doctors probably is on unlocked devices and is not encrypted. If you're following such practices, then you're violating HIPAA.

To fully comply with the regulations, you must follow many other requirements as well, yet many physicians are wholly unaware of them, let alone the PHI privacy policies in place where they see patients. Most healthcare organizations and hospitals take the HHS policies even further than physician practices, because they'll share the blame if you take PHI out of their systems and lose it. The fines for data loss or privacy violations can be enormous, so the policies of any hospitals with which you are affiliated most likely are even more stringent than those of the government. If you violate them, you could lose your privileges.

What am I getting at? You and your colleagues are under more scrutiny then ever before. As technology makes it easier for you to practice collaborative care, the penalties for doing so inappropriately are becoming more severe.

It's easy to be complacent where government and institutional policies are concerned. It behooves you, however, to completely understand your personal responsibilities under HIPAA to protect your patients' private health records and to be fully aware of the PHI exchange policies if you make rounds or work at a hospital in some capacity.

SOCIAL MEDIA AND HIPAA

Social media sites such as Facebook and LinkedIn can be great resources, but remember, they are public, not private. Posting any patient information on them violates the law. Private doctor-to-doctor sharing sites similar to Facebook exist where you can safely exchange PHI behind secure firewalls. Seek them out as alternatives.

And although your mobile devices offer ways to expand your practice and enhance your lifestyle, they're also potentially disastrous unless you take the proper steps to ensure they're secured.

Laptops, USB drives, smartphones, and tablet computers probably are the future of ambulatory medicine and remote healthcare. Ensure that your devices, as well as the way you use them, comply with current government regulations. And if you see patients at a hospital, be sure that the devices comply with the facility's PHI policies as well. Otherwise, you risk your practice and your livelihood.

You can find a complete guide to the government's rules concerning accessing PHI on portable devices at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf.

Send your feedback to medec@advanstar.com. Also engage at www.twitter.com/MedEconomics and www.facebook.com/MedicalEconomics.