Interview with... Kimberly Danebrock, RN, JD

Kimberly Danebrock, RN, JD, is a Senior Risk Management & Patient Safety Specialist for the Cooperative of American Physicians, Inc., CAPAssurance program. She has 30 years of combined experience in nursing, medical-legal, and risk management and patient safety. Ms. Danebrock develops and conducts risk management and patient safety educational presentations for physicians, residents, and office staff. She has a particular interest in the challenges of social media in a healthcare context, so Inside Medical Liability wanted to ask her about potential precautions—and possible benefits—of using social media in a professional practice.

Inside Medical Liability: What guidelines are available now (like books and research articles) for creating a social media policy?

Danebrock: There are many guides from professional organizations, such as the American Medical Association and the Federation of State Medical Boards, that provide great guidance on creating a social media policy. In addition, several organizations have their social media policy available online—such as the Cleveland Clinic, Kaiser Permanente, and the Mayo Clinic, which one can review and learn from. These are great places to start for anyone who is looking to implement policy on social media.

IML: How long have these associations been working on this?

Danebrock: That depends on the particular organization—and the size, and their ability to identify what their risks are, or have been. Some groups didn’t write these policies until they had issues and problems related to social media and the release of patient information.

But this effort goes back for some to 2008 and 2009; it’s been going on for years.

IML: It’s an evolving thing, though, isn’t it, since we keep seeing new social media?

Danebrock: Yes, and I think that’s a good thing. But unfortunately, physicians and hospital employees and most of us were not trained how to use these tools regarding healthcare. Actually, the real issue is that a lot of people use it in their personal lives, but those people don’t have to think about the federal privacy law, or the state privacy laws, or even about the ethical issues that people in medicine do.

IML: How do you teach those in healthcare that they need to separate their personal from their professional use of social media?

Danebrock: It is the recommendation of CAP, and from everything I have read on the topic, they should definitely work to keep these separate. For example, you would have a personal Facebook page for your friends and then a professional Facebook page for your practice.

On the professional Facebook page, you might include things like, “Hey, it’s time for flu vaccines.” Or maybe feature some educational materials. There are lots of different types of information you can post depending on your specialty. I have seen plastic surgeons feature notices like, “We’re having a Botox special.” You can post advice or information that is related to your business—as long as it doesn’t center around, or affect, patient privacy and issues related to how you represent yourself.

Your personal Facebook page should not include your patients.

You can post advice or information that is related to your business—as long as it doesn’t center around, or affect, patient privacy and issues related to how you represent yourself.
Social media in a practice and in healthcare is very important, although we have been slow to adapt in healthcare, because of privacy issues.

**IML:** What are the biggest risks for healthcare professionals, in using social media?

**Danebrock:** If the healthcare provider is using social media at work, the greatest risk is patient safety. There are documented cases of providers being negligent due to paying more attention to their personal electronic devices than the patient.

The other major risk is the accidental release of patients’ protected health information. The safe keeping of this private information is paramount to our patients. When information is released, that causes patients to lose trust in the provider—and the facility.

**IML:** How do HIPAA laws come into the picture?

**Danebrock:** The federal privacy rules identify 18 items that are called the “18 identifiers,” that, if released, would permit identification of a patient. While all of us think of those obvious identifiers, such as name or date of birth or medical record number, a lot of healthcare providers don’t realize that the 18th identifier is actually any other unique identifying number or characteristic.

So it’s really a catch-all. It could mean things such as a lesion, a tattoo, or an anomalous body part. Even if you didn’t show any written information, if you took a picture on a bodily area as I just described, and posted the photo on Facebook, you would actually have violated HIPAA laws.

One example of which I have heard, is of an EMT who brought in a patient who had a knife impaled in the abdomen. They brought the patient into the ER, and an x-ray was taken. Then, the x-ray was put up on the view box, and the EMT took a picture of the x-ray. They made sure they didn’t get the name or the date of birth in the photo, but then the x-ray got posted on Facebook. Obviously, knife in the abdomen is a pretty clear identifying characteristic.

Another example was when an ER doctor, after her shift, came home and posted, on her personal Facebook page, the general sense of the things she had seen that day in the ER. She ended up losing her hospital privileges and was fined by her medical board—for posting this general information about the patients she took care of that day.

So they considered it not only a violation of patient privacy, but also saw ethical issues in this instance. We are not supposed to actually post an overview of our day at work, as she did. It’s one thing if you’re talking to a class in medical school, and educating them, on a case, but it is another thing to go on your personal Facebook page and talk about the patients you saw that day. We have an ethical obligation not to do that to our patients.

**IML:** It will take a bit of time for people to get used to thinking this way, won’t it?

**Danebrock:** I think it’s no different from how we’ve been thinking, ever since the basic privacy laws of 1996. The issue is that we do so much on our electronic devices—without even thinking about it and we need to realize that the concept surrounding privacy is still the same.

Here is an example of why we need to be aware of what we do on our personal devices, and what can go wrong. A scrub tech had just graduated from a recent program, and he was very happy as it was the first day that he was going to be working as an OR tech on his own, without being a student. The physician in the room said, “Hey, let me take a picture of you. This is a great day.” He did that, and he then posted the picture on Facebook.

But what nobody realized is that we are so used to our environment, that no one noticed that behind him was the whiteboard with all of the patients’ names and what procedures they were having.

So when we educate staff on social media, what we say should always include such things as it’s never okay to put anything about a patient on social media.

**IML:** Are there any claims against physicians because of social media?

**Danebrock:** HIPAA and the federal privacy laws don’t provide a cause of action for a violation. But what is happening is that when a patient’s information is released, they’re starting to look at it as failing to meet the standard of care. That has indeed happened.