Bloomberg BNA

Health Law Resource Center™

Health Information

Attorneys Advise Caution in Using Doctor-to-Doctor Social Media Websites

By Mary Anne Pazanowski

Doctors regularly share information about patients with other doctors to aid them in diagnosing and treating those patients, but caution should be exercised when that consulting relationship goes online, health information and privacy attorneys told BNA.

Kirk J. Nahra, who specializes in health care, privacy, and information security issues as a partner at Wiley Rein LLP, in Washington, and Jennifer Breuer, a partner in Drinker Biddle's Chicago office and vice chair of the firm's health care practice group, told BNA that physician chat rooms and doctor-to-doctor social media sites can be beneficial, but also could lead to legal problems for health care providers. Elisabeth Belmont, corporate counsel of MaineHealth in Portland, Me., put it in stronger terms, calling the social media sites "a trap for the unwary."

Two of the more popular sites are Doximity, a 2010 start-up that claims to have 50,000 physician members, and Sermo, which launched in 2006 and says more than 125,000 physicians are registered. Both sites advertise that they verify that their members are, in fact, physicians, but Sermo permits members to post anonymously after registration. Both sites claim to facilitate secure communications between doctors.

Nahra said social media sites like these represent a "use of technology for beneficial purposes that is not without risk." Breuer agreed, saying that, for doctors in rural areas where there may not be many other physicians, the consulting opportunities presented by these sites are highly beneficial, but still troublesome.

HIPAA Protections

The most obvious problem with such sites is how to ensure that meaningful discussions between doctors can occur without violating state and federal privacy laws. Sharing information about patients on these sites may violate the privacy rule of the Health Insurance Portability and Accountability Act (HIPAA), they said.

HIPAA's privacy rule states that health care providers may not disclose individually identifiable patient information, designated in the rule as protected health information (PHI), to anyone other than the patient or his personal representative without the patient's prior written authorization.

There are a number of exceptions to the privacy rule. For example, sharing de-identified information, meaning information from which the identifying data has been removed or which provides no reasonable basis to identify the individual in accordance with privacy rule requirements, is permitted.

Posting de-identified patient information on the internet, however, is "not as blinded" as people would like to believe, Belmont said. The propriety of physicians posting comments concerning high-profile patients—the "Octomom," for example—or the victims of an accident that makes the national news, would be questionable even if the patient actually is not identified, given that the unique circumstances would make it possible to re-identify the patients, she said.

Treatment Exception

The privacy rule also contains an exception that allows physicians to share information about patients

with other physicians for treatment purposes. In response to allegations that a physician violated the privacy rule by disclosing PHI on a social media site, the physician could argue that she merely engaged in permitted treatment-related consulting activities.

Doctor-to-doctor social media sites represent a "use of technology for beneficial purposes that is not without risk."

Kirk J. Nahra, Wiley Rein

Website postings, however, fall "outside the traditional consult realm," according to Belmont. A physician seeking a consultation usually requests one from another physician within the same integrated delivery system, a specialist with whom he has a referring relationship, or a nationally recognized specialist, she said. How, Belmont asked, can the referring physician know whether the practitioner who responds to an online posting has the requisite expertise to provide proper advice?

Moreover, Belmont said, requesting a consult via a physician social networking site where the information is visible to potentially thousands of individuals may be inconsistent with the patient's expectations for how his medical information will be shared.

Additionally, application of the treatment exception depends on the type of treatment involved, Belmont said. The privacy rule does not preempt more stringent federal and state laws relating to the privacy of sensitive health information. For example, federal regulations relating to the confidentiality of alcohol and drug abuse patient records require a physician requesting a consultation for a substance abuse patient to have the patient's prior written permission to disclose such information.

Social media sites also are vulnerable to hacking and other security issues that could lead to loss of privacy protections for patient information posted on such sites, Belmont said.

Type of Site May Be Problem

Nahra and Breuer told BNA they would want to know the purpose of a doctor-to-doctor site before advising a health care provider to participate. Neither saw much of a problem with a site similar to LinkedIn, on which doctors would post only professional and contact information. They foresaw more problems with a chat room or Facebook-type site. Nahra's chief concern was that it would be too difficult to ensure that PHI was never posted on the site.

There are "a lot of random people" on Facebook, and a doctor cannot simply post patient information to the masses, he said. Even if the site provider promised that all its members were doctors, there still could be problems, he said, since the poster would not know every other site user.

A chat room made up of a smaller universe of doctors, for example, all physicians holding privileges at a specific hospital, might work better, Nahra said. The physicians likely would know each other, or at least could verify each other's identity and professional credentials. But, he asked, why even have such a site? Doctors call one another for consultations all the time. Each step in broadening the circle of physicians simply creates problems, Nahra said.

Cocktail Party?

Breuer analogized doctor-to-doctor websites to a "cocktail party," where physicians meet to network, form professional contacts, and discuss medical matters. These sites, like cocktail parties, could be used to develop mentoring relationships or obtain job-hunting assistance.

Online connections, however, present "a lot more risk" than a typical cocktail party, Breuer said. There may be no good way to verify that the person a doctor is speaking to in a chat room is qualified to consult on patient care. Breuer said she would urge doctors to verify the identity of the person they are consulting online. Although some doctor-to-doctor site providers advertise that they vet their members, that may not be sufficient to guarantee that only doctors are using the site, she said.

Verification Is Key

Thomas J. Smedinghoff, a partner at Edwards Wildman Palmer LLP, in Chicago, whose practice focuses on legal issues regarding privacy and online authentication, told BNA that verification is an important issue for doctor-to-doctor sites.

A physician using a site should ask two questions, he said: Who is the other person online, and how can his identity be proven? Before joining the site, the doctor should determine what the site operator is doing to verify its members' identities. Does the operator simply ask each registrant if he or she is a

doctor, then take their word for it, or does the operator have a more complex system in place?

Smedinghoff said the federal government uses four levels of assurance, ranging from simply asking a person for their identity to an investigation by a federal agency. A doctor-to-doctor site operator might take a middle ground. It could check with a state licensing agency to ascertain whether a registrant actually holds a license, or it could check medical school alumni records.

There still is the question of whether a registrant is the person he or she claims to be, Smedinghoff said. And, once the registrant's identity has been verified, there is the issue of whether the person who signs in under that name is the same person who registered. The latter can be addressed through user identification and passwords, Smedinghoff said. But those are not all that secure.

Absolute verification probably is out of the doctor-user's control, according to Smedinghoff. Users, therefore, should understand the risk that the person they are in contact with may not be a physician or have the expertise they claim, and decide whether it is appropriate to take that risk.

Licensure, Malpractice Questions

Breuer also warned of other legal issues that could arise from the use of doctor-to-doctor websites. For example, she said, doctors can practice only in states in which they are licensed. While most state licensing regulations recognize a consulting exception, that exception may not apply if the consultation request does not involve a specific identifiable patient, she said.

Doctors offering advice online also face malpractice risks, Breuer said, at least if the facts would support a finding of a doctor-patient relationship between the advisor and the patient. The advice-seeker, also, would be vulnerable to a malpractice suit, depending on the extent to which he relies on the online advice.

The advice-seeker's risk could be reduced through creating a one-on-one online relationship with another physician, as opposed to seeking advice from a community of health care providers, Breuer said. Proving the existence of a doctor-patient or consulting relationship likely would lessen the seeker's exposure under both malpractice law and HIPAA.

Belmont warned, also, that “plaintiff's lawyers are very savvy” about mining social media to find information that may be useful to support a medical malpractice claim. She added that internet postings, for example, fall outside the purview of most states' traditional peer review statutes, meaning that certain information that otherwise would be subject to statutory protections could become discoverable and be used against a physician in a malpractice lawsuit. This is another area where the law is lagging behind the adoption of the technology, Belmont said.

Nationwide Compliance Reduces Benefit

Even assuming a physician social networking site could be created that would not lead to inadvertent HIPAA violations, Nahra questioned whether the site would pose state compliance problems.

The privacy rule does not preempt more stringent state laws. For example, several states and localities expressly prohibit the release of information about a patient's HIV status. A doctor in a state that does not specifically prohibit such a disclosure (even in a de-identified format) may violate another state's law by sharing information about a patient who has HIV.

Formulating postings to ensure compliance with state laws eventually leads to a point where little benefit can be gained from a national website, Nahra said. He compared websites to electronic health records (EHRs). Ideally, EHRs are supposed to contain all of a patient's past health information to enable doctors who may be unfamiliar with a patient to quickly and efficiently access the patient's health history, thereby leading to a better outcome. State privacy laws, however, may restrict the type of information permitted in the records. The less information in the records, the less useful they are, Nahra said.