ARTICLES

Using Evidence of Industry Standard in Medical Record Breach Cases

By Bryan H. Heckenlively – February 17, 2016

There has been a surge in litigation in recent years surrounding unauthorized releases of data in electronic health records. Many of those lawsuits center upon whether the healthcare provider storing the data was negligent.

When a negligence claim against a healthcare provider goes to trial, the issue for the jury is whether the professional acted with the care expected of a reasonably careful provider acting under similar circumstances. To assist the jury in making that determination, the parties often present experts who describe what other healthcare providers actually do. *Osborn v. Irwin Mem'l Blood Bank*, 7 Cal. Rptr. 2d 101, 127 (Ct. App. 1992) ("[T]he professional standard of care is a function of custom and practice."). If the evidence is, for example, that it is standard practice across the country to prescribe a certain anti-inflammatory drug after surgery, that might lead the jury to conclude that a surgeon who did not prescribe it failed to exercise reasonable care. But a jury likely would not expect a surgeon to prescribe that medication if the evidence is that only a handful of other surgeons around the country do so.

The same should be true when the negligence claim against a healthcare provider is based on allegations of faulty data security. Doctors and hospitals increasingly collect and maintain significant amounts of sensitive data about their patients because they rely on that data in order to provide care. As a result, securing the data is within the scope of the services provided by the healthcare provider, and the provider's care in securing the data should be judged by the same standard as would be its care in providing services.

If that is the standard of care, healthcare providers should be permitted to introduce and ask the jury to rely on expert testimony about practices throughout the industry. That can be an enormously helpful tool to healthcare providers who acted carefully and made practical judgments consistent with those of their peers, but who nonetheless failed to prevent unauthorized access to data. And, because perfect security is impossible (or at least infinitely costly), any healthcare provider could find itself in that position.

Negligence Claims in Medical Data Breaches

When patients sue doctors, hospitals, or other healthcare providers for allowing unauthorized access to or failing to safeguard their medical information, they generally do so on theories of negligence. Often this is because the relevant state law offers a cause of action that refers to negligence. California's Confidentiality of Medical Information Act, for example, creates a private right of action against "any person or entity who has negligently released" medical information. Cal. Civ. Code § 56.36; *see also* Cal. Civ. Code § 56.101 ("Any provider of health care . . . who *negligently* creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." (emphasis added)). A Minnesota statute similarly gives patients a

private right of action against a healthcare provider who "negligently or intentionally requests or releases a health record." Minn. Stat. § 144.298. In Ohio, to take another example, the courts have recognized an independent tort "for the unauthorized, unprivileged disclosure to a third party of nonpublic medical information that a physician or hospital has learned within a physician-patient relationship." *Sheldon v. Kettering Health Network*, 40 N.E.3d 661, 672 (Ohio Ct. App. 2015).

Many plaintiffs sue on theories of common-law negligence in addition to or instead of bringing healthcare-specific negligence claims. *See, e.g.*, Court's Ruling on Submitted Matter, *Lozano v. Regents of Univ. of Cal.*, No. BC505419 (Cal. Super. Ct. Apr. 15, 2014), 2014 WL 10706721 (the author represented the Regents of the University of California in this matter); Class Action Complaint, *Fodda v. Sutter Med. Found.*, No. BC474428 (Cal. Super. Ct. Dec. 6, 2011); *see also Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C.*, 102 A.3d 32, 49 (Conn. 2014) (finding common-law negligence claim for breach of healthcare provider's duty of confidentiality not preempted by HIPAA); *I.S. v. Wash. Univ.*, No. 4:11CV235SNLJ, 2011 WL 2433585 (E.D. Mo. June 14, 2011) (same).

The Professional Negligence Standard

The question in these cases becomes how to define the standard of care—a question that is relevant to summary judgment and expert discovery and particularly important to the jury instructions and expert evidence presented at trial. There are two competing approaches. One option is to treat this as an issue of general negligence and apply the reasonably prudent person standard. Another is to classify it as professional negligence subject to the specialized standard of care developed in malpractice cases.

In theory, the difference between these two possibilities should not be significant. As the California Supreme Court has explained: "Because application of [due care] is inherently situational, the amount of care deemed reasonable in any particular case will vary, while at the same time the standard of conduct itself remains constant, i.e., due care commensurate with the risk posed by the conduct taking into consideration all relevant circumstances." *Flowers v. Torrance Mem'l Hosp. Med. Ctr.*, 884 P.2d 142, 144 (Cal. 1994).

As a practical matter, there is a significant difference. Rather than permitting a patient to lead the jury through an unguided analysis of what the provider should have done to protect its records, the law and associated jury instructions regarding professional negligence expressly require the jury to tether its consideration of due care to what other similarly situated providers would do. That specific standard injects a measure of practicality into the analysis by forcing the jury to consider whether a reasonable provider really would have adopted the hypothetical security measures proposed by the plaintiff.

To give a concrete example, the standard instructions for an ordinary negligence case in California tell the jury that it may "consider customs or practices in the community in deciding whether [the defendant] acted reasonably," but that "[c]ustoms and practices do not necessarily

determine what a reasonable person would have done" and that it is up to them to "consider whether the custom or practice itself is reasonable." CACI 413. But the usage notes make clear that "[a]n instruction stating that evidence of custom is not controlling on the issue of standard of care should not be given in professional malpractice cases in which expert testimony is used to set the standard of care." *Id.* (citing *Osborn*, 7 Cal. Rptr. 2d at 124). That is because the standard of care for medical negligence is "the level of skill, knowledge, and care in diagnosis and treatment that other reasonably careful [medical practitioners of the same type] would use in the same or similar circumstances." CACI 501.

Applying the Professional Negligence Standard to Data Security

In states where medical malpractice reform statutes have broadly defined what is "professional negligence" as opposed to ordinary negligence in the healthcare context, there is a straightforward argument that the professional negligence standard should apply to claims of negligent record storage. In California, to take one example, professional negligence includes any situation where "the injury for which damages are sought is directly related to the professional services provided by the health care provider" or directly related to "a matter that is an ordinary and usual part of medical professional services." *Cent. Pathology Serv. Med. Clinic, Inc. v. Superior Court*, 832 P.2d 924, 930–31 (Cal. 1992). In Texas, to take another, "[i]f the act or omission that forms the basis of the complaint is an inseparable part of the rendition of health care services, or if it is based on a breach of the standard of care applicable to health care providers, then the claim is a health care liability claim." *Sloan v. Farmer*, 217 S.W.3d 763, 767 (Tex. App. 2007).

In modern practice, storing and securing electronic patient information is a critical part of providing patient care. The federal government has recognized as much by offering incentives to medical practitioners and hospitals that implement them. And healthcare providers must safeguard electronic records they keep on their patients, just as they would with paper charts. Thus, it seems clear that taking measures to safeguard the electronic records is sufficiently related to providing healthcare services to meet the definitions in those statutes. *Cf. Sloan*, 217 S.W.3d at 768 ("Maintaining the confidentiality of patient records is part of the core function of providing health care services."); *Francies v. Kapla*, 26 Cal. Rptr. 3d 501, 505 (Ct. App. 2005) (finding that disclosure of patient's health condition to his employer gave rise to a claim of professional negligence).

Even without the benefit of a statutory definition like California's or Texas's, it should be apparent that maintenance of electronic health records is subject to a professional negligence standard. The professional negligence standard is meant to ensure that, when a matter is beyond the common understanding of a layperson, the jury relies on only expert testimony regarding the *actual* standard of care in the industry. *Osborn*, 7 Cal. Rptr. 2d at 128 ("[P]rofessional prudence is defined by actual or accepted practice within a profession, rather than theories about what 'should' have been done."). Proper storage of electronic health records is, clearly, not a matter of common knowledge. It depends on expertise both in technical security measures—encryption and authentication technology, for example—and in the delivery of medical care, in order to

ensure that records are secure but not so secure that they cannot be accessed when needed to take care of patients.

Introducing Evidence of Industry Standards

As this discussion suggests, expert testimony regarding best practices in the industry for storing electronic medical records should be welcomed because it will "help the trier of fact" determine whether a healthcare provider met the standard of care. Fed. R. Evid. 702; *see also Alef v. Alta Bates Hosp.*, 6 Cal. Rptr. 2d 900, 907(Ct. App. 1992) (recognizing that the issue is whether the expert's "testimony would be likely to assist the jury in the search for truth").

That type of expert testimony can be powerful for a healthcare provider facing a negligence claim. When a patient's record is compromised, it is fairly easy for his or her lawyer to identify one or more hypothetical security measures that the healthcare provider had not adopted because providers cannot adopt every single theoretically possible security measure. Some measures might not be technically practical or economically feasible, and, critically, some measures might put patients at unnecessary risk by making records so secure that medical personnel cannot access them when needed. For example, requiring a retinal scan to access patient records might prevent a hacker from breaking into a record with a stolen password, but it might also prevent an emergency room physician from having immediate access in an emergency. In that situation, although the healthcare provider could explain to the jury how it balanced security with patient care needs, it would be much more effective to present expert testimony that other similarly situated providers have made the same decision—that the rest of the industry also has chosen not to implement retinal scanners.

If there is no countervailing expert testimony, that type of industry standard evidence may be conclusive. In the *Osborn* case cited earlier, the court affirmed a judgment notwithstanding the verdict for just that reason. That case involved a different issue, but still one of professional negligence: the standard of care for blood banks in the 1980s screening blood for AIDS. The plaintiff's expert testified that the defendant blood bank failed to perform certain tests that he and others in the field believed should have been required at the time. There was, however, uncontradicted evidence presented by the defense that no blood bank in the country was performing those tests. That, according to the court, meant that "there was no substantial evidence that failure to conduct the tests" fell short of the standard of care. *Osborn*, 7 Cal. Rptr. 2d at 123–28.

With that in mind, healthcare providers defending against negligence claims related to electronic health record storage would be well served to develop expert testimony about comparable practices of other providers and to extract concessions, if possible, from the plaintiff's expert that his or her testimony is normative and not drawn from the actual practices of comparable providers. Plaintiffs, conversely, might seek out experts who can identify measures widely adopted by other providers but not present to protect their own records.

Conclusion

Applying the professional negligence standard to claims based on unauthorized access to electronic medical records is the correct result doctrinally, and it opens the door to introducing potentially powerful expert testimony regarding the practices of other participants in the industry. Although the discussion here has focused on healthcare providers' medical records, one might make a similar argument for other professionals who use and must maintain data about their clients or customers in order to provide professional services. That could be a useful tool at trial for law firms, accounting firms, financial advisory firms, and other professionals who are at risk of data breaches.

Keywords: litigation, trial evidence, electronic medical records, data security, negligence, standard of care, industry practices, expert testimony

Bryan H. Heckenlively is a litigator with Munger, Tolles & Olson LLP in San Francisco, California.