MANAGED CARE OUTLOOK

The Insider's Business Briefing on Managed Healthcare

Volume 27, Number 16 • August 15, 2014

Data Breach Litigation: Is West Virginia a Trailblazer?

Tatiana Melnik

Data breaches continue to be in the spotlight, and business associates continue to be a common cause. Thanks to the Health Information Technology for Economic and Clinical Health (HITECH) Act's reporting requirements, health care-related data breaches impacting 500+ individuals must be publicly disclosed, and the name of the business associate that caused the breach also must be revealed.

As of July 7, 2014, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights' (OCR's) public database of data breaches impacting 500+ individuals listed 1,059 breaches impacting close to 32 million individuals.[1] Breaches impacting less than 500 individuals are also reportable. On May 20, 2014, the OCR submitted a report to Congress detailing the statistics related to these breaches for years 2011–2012, with brief highlights of data for 2009 and 2010.[2] (See Figure 1)

But, remedies for victims of data breaches continue to be elusive for a number of reasons. Most prominently among these is the fact that victims rarely meet the standing requirement because they cannot demonstrate an injury. That is, to successfully bring a lawsuit, a plaintiff must have standing — a right to bring a claim. As the West Virginia Supreme Court in *Tabata v. Charleston Area Medical Center, Inc.* explained:

> Standing is comprised of three elements: First, the party attempting to establish standing must have suffered an "injury-in-fact" — an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent and not conjectural or hypothetical. Second, there must be a causal connection between the injury and the conduct forming the basis of the lawsuit. Third, it must be likely that the injury will be redressed through a favorable decision of the court.[3]

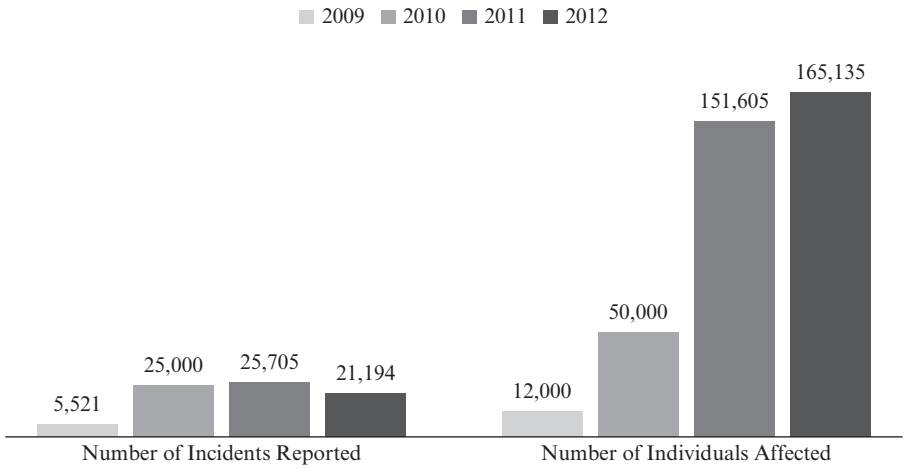
Many data breach-related cases fail because plaintiffs cannot demonstrate an injury-in-fact; with few exceptions, 'hurt feelings' because a person's medical records were disclosed online do not form a sufficient basis for a claim.[4] To demonstrate a cognizable injury, plaintiffs must demonstrate some *concrete* injury, such as identity theft, loss of a job, and so forth. In many data breach cases, victims cannot show any actual injury, other than their fear of becoming a victim of identity theft.

However, it appears, in West Virginia at least, that courts are willing to consider possible damages without an immediate risk of harm.

Tabata v. Charleston Area Medical Center, Inc. and the Involvement of a Business Associate

The *Tabata* litigation stems from a data breach, which exposed plaintiffs' information online from September 2010 thru February 2011 when a database was formatted incorrectly, permitting access to the information without a password.[5] According to a press report by WSAZ in West Virginia, the issue

Figure 1: HHS OCR, Breaches Affecting Fewer than 500 Individuals from 2009–2012[1]



[1]HHS, OCR, Report to Congress on Breach Notification Program: 2011–2012 Report to Congress on the Breach Notification Program, www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreptmain.html (last visited July 7, 2014).

came to light when Lorrie Lane reported to the West Virginia Attorney's Office that her "brother-in-law was searching for a family friend's address for a wedding invitation when he conducted a Google search of her name and found [her medical] records."[6]

In February 2011, following the notification from the West Virginia Attorney General, the Charleston Area Medical Center, Inc. and CAMC Health Education and Research Institute, Inc. (collectively, "CAMC") notified the plaintiffs that a database containing "names, contact details, Social Security numbers, and dates of birth of 3,655 patients, along with certain basic respiratory care information," was placed online.[7] According to the data breach database maintained by OCR, a business associate — Xforia Web Services — was involved in the incident.[8]

The plaintiffs alleged that "this information could be exposed if someone were to conduct an advanced internet search."[9] Plaintiffs raised a number of state-based causes of action, including (1) breach of duty of confidentiality; (2) invasion of privacy — intrusion upon the seclusion; (3) invasion of privacy — unreasonable publicity into the plaintiffs' private lives; and (4) negligence. Plaintiffs also sought class certification.

The lower court denied class certification because "[d]iscovery revealed that the [plaintiffs and CAMC were] not aware of any unauthorized and malicious users attempting to access or actually accessing their information, [were] not aware of any of the 3,655 affected patients having any actual or attempted identity theft[, and the plaintiffs had] not suffered any property injuries or sustained any actual economic losses."[10] Among other things, the lower court ruled that the plaintiffs lacked "standing to bring their claims because they have failed to show that they have suffered a concrete and particularized injury that is not hypothetical or conjectural."[11]

In reversing the lower court's decision, the West Virginia Supreme Court ruled that allegations of breach of confidentiality and invasion of privacy where sufficient to meet the injury in fact requirement for purposes of standing. With respect to breach of confidentiality, the Court explained that "a patient does have a cause of action for the breach of the duty of

confidentiality against a treating physician who wrongfully divulges confidential information … and this legal interest is concrete, particularized, and actual."[12] Further, the Court explained that, "[w]hen a medical professional wrongfully violates this right, it is an invasion of the patient's legally protected interest [for which plaintiffs'] and the proposed class members have standing to bring a cause of action[.]"[13]

Similarly, the Court held that plaintiffs have a cause of action for invasion of privacy and this interest is concrete, particularized, and actual.[14] Additionally, the Court held that a "declaration in an action for damages founded on an invasion of the right of privacy, to be sufficient on demurrer, need not allege that special damages resulted from the invasion."[15] As a result, the West Virginia Supreme Court concluded that the class may be certified despite explicitly recognizing that there was "no evidence of unauthorized access of [plaintiffs'] personal and medical information, no evidence of actual identity theft, and no evidence of economic injury arising from the alleged wrongdoing."[16]

Concluding Thoughts

Medical providers and others who are entrusted with protected health information must continue to pay close attention to both federal and state-based litigation surrounding data breaches and adjust their calculus accordingly. While, in the end, plaintiffs may lose because they cannot prove damages, defending against a class action is not an inexpensive endeavor. Additionally, while it is true that this case is based on West Virginia law, the breach of confidentiality and invasion of privacy causes of action are grounded in common law and are recognized in every state in one form or another. As data breaches continue to dominate the news, other state courts may be persuaded by the analysis of the West Virginia Supreme Court.

Medical providers should also carefully evaluate their partners and ensure that appropriate damages caps, indemnification, and insurance language is included in both master services and business associate agreements. Interestingly, in the *Tabata* case, while the breach report with OCR lists that Xforia Web Services was involved in the incident, the company is not a defendant in the litigation. As such, providers should take the time to carefully evaluate the damages caps, indemnification, and insurance provisions in their agreements because, in the end, they will likely bear the brunt of the litigation.

Tatiana Melnik is an attorney focusing her practice on information technology, health care, data privacy and security, regulatory compliance, and general business matters. Ms. Melnik regularly writes and speaks on HIT legal issues, including cloud computing, HIPAA/HITECH, BYOD, and data breach reporting requirements. She is a managing editor of the Nanotechnology Law and Business Journal and a former member of the Michigan Bar Information Technology Law Council. Ms. Melnik is admitted to practice in Florida and Michigan. Ms. Melnik holds a JD from the University of Michigan Law School, a BS in Information Systems, and a BBA in International Business, both from the University of North Florida. She can be reached by phone at 734/358-4201 or by email at tatiana@melniklegal.com. ■

Endnotes:

1. *See* HHS Office of Civil Rights, Breaches Affecting 500 or More Individuals, www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (last visited July 7, 2014).
2. For more detailed data on years 2009 and 2010, *see* HHS, OCR, Report to Congress on Breach Notification Program: 2009-2010 Report to Congress on the Breach Notification Program, www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachrept.pdf (last visited July 7, 2014).
3. Tabata v. Charleston Area Medical Center, Inc., No. 13-0766, Case No. 11-C-524 (W.Va. S.Ct. May 28, 2014), available at melniklegal.com/av/2014_Tabata_v_CAMC_W-0766.pdf.
4. In some circumstances, given the type of information revealed, 'hurt feelings' can form the basis of a cognizable injury. Many states recognize the four general categories of 'invasion of privacy' torts, which include (1) intrusion upon seclusion (*i.e.*, invading plaintiffs' physical solitude or seclusion); (2) public disclosure of private facts; (3) false light in the public eye (analogous to the law of defamation); and (4) appropriation

(*i.e.*, commercial exploitation of the property value of one's name or likeness). *See e.g.*, Prosser, The Law of Torts (4th ed. 1971). In the case of defamation, many states recognize defamation "per se," which has grounds in common law. In these cases, damages are presumed if the defamatory statement, in general, (1) impugns a person's professional; (2) alleges that an unmarried person is unchaste (*e.g.*, is sexually active); (3) alleges that a person is infected with a sexually transmitted disease; or (4) alleges that the person has committed a crime of moral turpitude (*e.g.*, theft or fraud). *See e.g.*, Rest. (2d) of Torts, §§ 570-574; Cal. Civ. Code § 44.

5. *See* WSAZ, UPDATE: Security Breach Reported at CAMC; Thousands of Patients Affected, WSAZ News Channel 3, Feb. 16, 2011, www.wsaz.com/news/headlines/needs_checkedAG_to_Hold_Presser_to__116232619.html.
6. *Id*.
7. *Tabata*, No. 13-0766 at 1.
8. HHS, Breaches Affecting 500 or More Individuals, www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (last visited July 7, 2014).
9. *Id*.
10. *Id*. at 2-3.
11. *Id*. at 3. The lower court also denied class certification because it found that the plaintiffs failed to meet "their burden of showing commonality, typicality, and predominance of common issues of law or fact for the purposes of class certification under Rule 23 *West Virginia Rules of Civil Procedure*." *Id*.
12. *Tabata*, No. 13-0766 at 5-6.
13. *Id*. at 6.
14. *Id*. at 7.
15. *Id*.
16. *Id*. at 13.