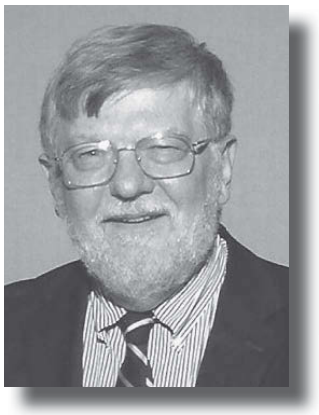
The Costs of Medical Privacy Breach

Reprinted with the permission of *MDAdvisor*, A Journal for the New Jersey Medical Community

by John Zen Jackson, Esq.



John Zen Jackson, Esq.

"Whatever, in connection with my professional practice, or not in connection with it, I see or hear in the life of men, which ought not be spoken of abroad, I will not divulge as reckoning that all such should be kept secret."

The Hippocratic Oath

The stakes for failing to adhere to adequate protections for patient medical confidentiality keep getting higher. In addition to the already frightening scope of penalties and problems that might follow a breach of the HIPAA Privacy Rule, a recent case in Indiana dramatically highlights the increasing risk to a healthcare provider from the wrongful use and disclosure of a patient's healthcare information. In connection with the HIPAA Privacy Rule, such information and data are termed Protected Health Information (PHI).

On April 14, 2003, compliance with the HIPAA Privacy Rule became mandatory for most covered entities. The Office for Civil Rights (OCR)—the enforcement arm for the Department of Health and Human Services—began to accept complaints involving the privacy of personal health information in the American healthcare system. At that time, it was OCR's stated intention to pursue enforcement activities through an approach initially emphasizing guidance and technical assistance.[1]

However, the agency had more coercive tools available to it and with the passage of time it has been employing these more coercive tools with significant impact on healthcare providers. The potential penalties for HIPAA non-compliance range from $100 to $50,000 for violations that occur in the absence of willful neglect to penalties starting at $50,000 in the circumstances of willful neglect. As has been recently noted, for the two-year period of 2011–2012, approximately 15 million individuals had their protected health information compromised through various HIPAA breaches. OCR had assessed penalties of some $3.5 million in 2013 and more than $7 million through the first half of 2014.[2]

With the enactment and implementation of the Health Information Technology for Economic and Clinical Health Act (HITECH) in 2009, business associate liability for HIPAA breaches was expanded, and state attorneys general received the power to bring HIPAA enforcement actions. There have been several settlements reached in actions brought by the state attorneys general.[3]

Breach of Privacy Violations and Penalties

The Department of Justice in conjunction with the FBI has responsibility for dealing with criminal violations. It is a federal criminal offense for a person to commit any of the following three acts:

1. to knowingly and in violation of the regulations use or cause to be used a unique health identifier
2. to knowingly and in violation of the regulations obtain individually identifiable health information relating to an individual
3. to knowingly and in violation of the regulations disclose individually identifiable health information to another person[4]

The penalties for a criminal violation depend on the circumstances of the wrongful use and disclosure. The penalty may be a fine of not more than $50,000 with imprisonment for not more than one year, or both, with an enhancement of the penalty if the offense is committed under false pretenses with a fine of up to $100,000, imprisonment for not more than 5 years, or both. Most severely, if the offense is committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm, the offender can be fined not more than $250,000, imprisoned not more than10 years, or both.[5]

The first criminal case was brought in 2004 in the Western District of Washington. It involved a phlebotomist who obtained a cancer patient's personal information from his health record and used it to fraudulently obtain four credit cards, making charges of thousands of dollars in the patient's name. The phlebotomist received a 16-month prison sentence.[6] Criminal prosecutions, although rare in comparison to the civil enforcement by OCR, continue to occur. In August 2014, a former hospital nurse entered a plea of guilty in the Eastern District of Texas to wrongful disclosure of protected health information for personal gain. In February 2015, he was sentenced to 18 months in federal prison.[7]

An obligation to preserve patient confidentiality has long been part of licensing schemes and a basis for professional disciplinary actions. Violations of HIPAA regulations have been the basis for a number of physician disciplinary proceedings based on a finding of "professional misconduct." The New Jersey State Board of Medical Examiners is empowered to ground disciplinary decisions in the violation of any state or federal statute or regulation that the Board is responsible for administering.[8] Reprimands have been issued in New Jersey and elsewhere.[9]

Private Lawsuits for Breach of Privacy Damages

Until 2006, multiple court decisions had repeatedly rejected individual patients' attempts to base a claim for compensation on breach of the HIPAA regulations. However, this absence of the right to bring private civil damage lawsuits under the HIPAA Privacy Rule has proven to be of limited protection. The potential for a renewed concern regarding HIPAA violations forming the basis for tort claims was recognized.[10] Rather than basing the tort claim on the violation of any provisions of the HIPAA regulations, a claim was formulated as a breach of the common law protection of patient confidentiality with the HIPAA Privacy Rule providing evidence of the appropriate standard of care that was to be observed and which had been breached.

Starting with the 2006 North Carolina decision of *Acosta v. Byrum*[11] there has been an increasing groundswell of cases recognizing state law claims of violation of physician-patient confidentiality and privacy arising out of conduct that violates the HIPAA Privacy Rule. A similar conclusion has been reached in Missouri[12] Minnesota,[13] Tennessee,[14] West Virginia[15] and Connecticut.[16] The Connecticut decision from mid-November 2014 even allowed use of the breach of medical confidentiality as protected by the HIPAA Privacy Rule to provide a basis for a class action.

In addition to demonstrating a duty of confidentiality and breach of that duty, a plaintiff asserting the wrongful disclosure of patient information must establish that the breach proximately caused the alleged damages being claimed. Compensatory damages in an action for wrongful disclosure may include recovery for emotional distress, the costs of medical or psychiatric treatment for emotional injuries caused by the disclosure and lost wages or loss of employment. If a patient relies on an invasion of privacy theory, then his or her recovery generally will be based on emotional suffering and injury to the patient's reputation. A plaintiff may not have to allege a physical injury in order to recover for the emotional distress allegedly caused by the disclosure of confidential medical information. In the absence of catastrophic consequences from the wrongful disclosure, the extent of recovery in these cases has been relatively limited. Jury awards were frequently only a few thousand dollars; although, there are some verdicts in excess of $100,000.[17]Not surprisingly, there have been some verdicts that have included punitive damage awards because of aggravating circumstances.[18]

The Indiana Case: A Clarion Call

Tort exposure arising from conduct in breach of the HIPAA Privacy Rule took on a new dimension with the decision of the Indiana Court of Appeals upholding a jury verdict in favor of plaintiff for $1.8 million. This verdict was reduced by 20 percent for an amount of injury attributable to the conduct of a non-party, with a resulting final award of $1.44 million.

In *Walgreen Co. v. Hinchy,*[19] the trial court permitted the use of HIPAA as evidence of the standard of care for a pharmacist's duty of confidentiality and privacy regarding a patient's protected health information. Pharmacies are considered "covered entities" under HIPAA[20] and, similar to physicians, have a regulatory obligation to maintain confidentiality of patient information.[21]

Plaintiff Hinchy had been having an on-and-off sexual relationship with a Mr. Peterson. Hinchy filled all of her oral contraceptive prescriptions at a Walgreen pharmacy. While Peterson was seeing Hinchy, he also began dating a Walgreen pharmacist named Withers. At some point in the relationship, Hinchy became pregnant with Peterson's child. Later, Peterson learned that he had contracted genital herpes. After the birth of the child, Peterson informed Withers about both the baby and the possible exposure to herpes. Withers accessed the Walgreens prescription profile for Hinchy to see if she could find any information regarding treatment for sexually transmitted diseases. In the ensuing litigation, Withers claimed that she did not look for information regarding birth control prescriptions and did not reveal any of the information that she had accessed to anyone. The jury did not accept the pharmacist's version of events.

Peterson had an exchange of text messages with Hinchy in which he berated her regarding the failure to refill her oral contraceptive prescriptions and claiming to have a printout of the record. His remarks were in connection with an attempt to rebuff claims for child support in connection with a paternity lawsuit. Concerned as to how Peterson had this information, Hinchy contacted a Walgreens branch but was informed that there was no way to track whether her records had been accessed. Hinchy took no further action at that time.

About a year later, however, Peterson sent a gift to his son with a return address on the package that Hinchy did not recognize. Through an Internet search, she linked the address with Withers and learned that Peterson and Withers had married. She also learned that Withers was a pharmacist at the local pharmacy where Hinchy filled her prescriptions. Hinchy contacted her local pharmacy to report her suspicions. The Walgreens investigation confirmed that in violation of HIPAA, Withers had accessed Hinchy's prescription information without consent.

continued on page 30

continued from page 29

Hinchy's lawsuit had several counts of wrongdoing against Withers and claims of vicarious responsibility against Walgreens for Withers' actions, as well as direct claims based on negligent supervision and training of its employee. Summary judgment was denied, and the case was presented to a jury in July 2013. The jury returned a verdict in favor of the patient and found that the total amount of damages suffered by Hinchy was $1.8 million, that Peterson even though a non-party who was not sued was responsible for 20 percent of the damages and that Walgreen and Withers were jointly responsible for the remaining 80 percent. (The issues involving the employer's vicarious liability and defenses based on conduct outside the scope of the pharmacist's employment warrant fuller discussion than this article permits.[22])

In its review on appeal, the intermediate Indiana Court of Appeals easily found a basis for liability in the negligent breach of a duty of confidentiality on the part of the pharmacist and that Hinchy had provided evidence of resulting damages. The court then rejected the contention that the verdict was excessive in amount. It noted that there was the following evidence of Hinchy's damages:

- The pharmacist had learned about Hinchy's private health information, including her social security number, and then shared that information with Peterson, who then shared the information with at least three other people.
- Hinchy's father learned about her use of birth control, that she had herpes and that she had stopped taking birth control shortly before becoming pregnant.
- Hinchy testified that she experienced mental distress, humiliation and anguish as a result of the breach. She stated that she was upset, crying and feeling "completely freaked out...." She felt "violated," "shocked" and "confused."
- The disclosure led to Peterson berating Hinchy for "getting pregnant on purpose" and eventually extorting Hinchy by threatening to release the details of her prescription usage to her family unless she abandoned her paternity lawsuit.
- Hinchy testified that she experienced uncontrollable crying that affected her ability to care for her child, went to a counselor to address the emotional toll of the privacy breach, experienced a general distrust of all healthcare providers and felt a persistent and continuous loss of "peace of mind."
- Hinchy also testified that she was now taking Celexa, an antidepressant, which costs $75 per month. Before the breach, she had taken a weaker antidepressant intermittently and had not taken it for more than one year before the breach.[19]

In support of its argument as to excessive damages, the defendant Walgreens contended that: 1) Hinchy did not have a physical injury or condition resulting from the breach, 2) Hinchy had no lost wages as a result of the breach and 3) Hinchy did not offer any testimony from a medical professional or counselor supporting her claim of emotional distress.[19] The court viewed these arguments as a request that it reweigh the evidence, which it would not do. Accordingly, the verdict was upheld. Defendant Walgreens requested that the intermediate Court of Appeals reconsider its ruling. That request was denied as was the Walgreen petition for further review by the Indiana Supreme Court. [23]

Protective Steps

The catastrophic potential of such verdicts becoming wide spread is underscored by the likely limitations of insurance coverage. Breach of medical confidentiality claims are not automatically encompassed by the protection of medical malpractice liability insurance. Some policies utilize the concept of "medical incident" arising out of or resulting from professional services to preclude coverage for a breach of medical confidentiality.[24] Even when the conduct giving rise to the claim occurs during the performance of professional services so as to come within the definition of "medical incident," coverage may be denied based on policy exclusions for conduct that violates a statute[25] or based on the characterization of the conduct as an intentional act.[26]

The insurance industry has responded by offering coverage for different aspects of the costs or liabilities that arise from breach of medical confidentiality or from data breaches involving personally identifiable information such as Social Security numbers or dates of birth. The area of "cyber risk" in particular has seen expansion as stand-alone or supplemental coverage. In light of the expanding exposure, these new insurance products are well worth evaluating to assess whether the insuring clauses, definitions and exclusions provide meaningful protection. The cost of such coverage needs to be assessed in terms of the scope of the offered coverage and the potentially substantial monetary penalties or damage awards that can be imposed.

Another fundamental protective step is having in place appropriate policies and procedures for handling confidential patient information and PHI, along with adequate training on privacy concepts and practices for new employees and staff at the start of employment. Furthermore, there should be periodic retraining of HIPAA standards to refresh or update staff. The lack of such basic orientation and education by the employer creates significant vulnerability to liability for various regulatory and tort violations.

In addition to policies and procedures for the healthcare professional's staff, it is important to have in place so-called Business Associate Agreements with non-workforce personnel and non-employees who nonetheless perform certain functions or activities that involve the use or disclosure of PHI on behalf of, or in providing services to, a covered entity. Such agreements place an obligation on the business associate to adhere to the HIPAA practices and policies of the healthcare professional.

Similarly, making provisions for audits of electronic records to identify inappropriate or suspicious activities or access should be considered by the prudent medical practice or its managers. While audits may not actually be a protective step to prevent a privacy breach, audits permit earlier recognition of a problem and allow for attempts to mitigate and ameliorate any damage.

Lastly, the implementation of the exquisitely simple step of encryption protocols for laptops and other portable data devices cannot be overemphasized. Encryption should not be ignored because of the powerful protection it can provide against inadvertent disclosures. Encryption makes electronically stored data inaccessible or unreadable. Indeed, if encrypted, lost PHI data on a misplaced or lost laptop may well not even be a breach that needs to be reported under HIPAA.[27] While encryption of ePHI can be a powerful source of comfort, the protocols to do so must be done correctly and periodically updated as the technology changes and advances.

It is important for all healthcare professionals to be aware that although HIPAA does not provide a private cause of action, an action for breach of confidential information is likely recognized under state law, and HIPAA may be used as evidence of the appropriate standard of care. Beside the tort exposure, the regulatory penalties can be devastating. Moreover, law enforcement has embraced the notion that the days when medical employees could snoop around patient charts for "juicy" information to share outside the office or hospital are very much gone. Such conduct subjects the offender to criminal prosecution and imprisonment.

About the author

John Zen Jackson, Esq. is certified by the Supreme Court of New Jersey as a civil trial attorney and is a Fellow of the American College of Trial Lawyers. He is a partner in the law firm of McElroy, Deutsch, Mulvaney & Carpenter, LLP and a member of the firm's Health Care Practice Group.

Footnotes

[1]68 Fed. Reg. 18885 (Apr. 17, 2003).

[2]Tamburello, L. M. (2014, Fall). Practical lessons from HHS's 2011-2012 report on HIPAA breaches of unsecured PHI. *MDAdvisor, 7,* 4, E37–E41.

[3]*See, e.g.,* Healey, M. (2014, July 23). *Women & Infants Hospital to pay $150,000 to settle data breach allegations involving Massachusetts patients.*www.mass.gov/ago/news-and-updates/press-releases/2014/2014-07-23-women-infants-hospital.html; Jepsen, G. (2010, July 6). *Attorney General announces health net settlement involving massive security breach compromising private medical and financial information.* www.ct.gov/ag/cwp/view.asp?A=2341&Q=462754; London, S. (2011, January 26). *Court approves Attorney General HIPAA settlement with health insurer.* http://ago.vermont.gov/focus/news/court-approves-attorney-general-hipaa-settlement-with-health-insurer.php.

[4]42 U.S.C. § 1320d-6(a).

[5]42 U.S.C. § 1320d-6(b).

[6]*United States of America v. Richard W. Gibson*, 2004 WL 2237585 (W.D.Wash.)

[7]U.S. Attorney's Office, Eastern District of Texas. (2015, February 17). *Former hospital employee sentenced for HIPAA violations.* www.justice.gov/usao-edtx/pr/former-hospital-employee-sentenced-hipaa-violations.

[8]N.J.S.A. 45:1-21(h).

[9]*See, e.g.,* New Jersey State Board of Medical Examiners. (2012, March 14). *In the matter of Nikhil S. Parikh, M.D,* License No. 25MA04165700; Rhode Island Board of Medical Licensure and Discipline. (2011, April 13). *In the matter of Alexandra Thran, M.D.* www.health.ri.gov/discipline/MDAlexandraThran.pdf.

[10]Jackson, J. Z. (2008, Winter). Renewed concern for tort actions based on HIPAA violations. *MDAdvisor, 1,*1, 14–17.

[11]638 S.E.2d 246 (N.C. App. 2006).

[12]*I.S. v. Washington Univ.,* 2011 U.S. Dist. LEXIS 66043, 2011 WL 2433585 (E.D. Mo. June 14, 2011); *K.V. v. Women's Healthcare Network, LLC,* 2007 U.S.Dist. LEXIS 102654, 2007 WL 1655734 (W.D. Mo. June 6, 2007).

[13]*Yath v. Fairview Clinics, N.P.,* 767 N.W.2d 34 (Minn. App. 2009).

[14]*Harmon v. Maury County,* 2005 U.S. Dist. LEXIS 48094, 2005 WL 2133697 (M.D. Tenn. Aug. 31, 2005).

[15]*Tabatha v. Charlestown Area Medical Center,* 759 S.E.2d 459 (W.Va. 2014); *R.K. v. St. Mary's Medical Center,* 735 S.E.2d 715 (W.Va. 2012), *cert. denied,* 133 S.Ct. 1738 (2012).

[16]*Byrne v. Avery Center for Obstetrics and Gynecology,* 102 A.3d 32 (Conn. 2014); *Doe v. Southwest Cmty. Health Ctr., Inc.*, 2010 Conn. Super. LEXIS 2167, 2010 WL 3672342 (Conn. Super. Ct. Aug. 25, 2010).

[17]*Huff v. Sabers, D.M.D.*, JVR No. 1104060077, 2010 WL 7058366 (Fla.Cir.Ct.); *M.L. v. St. John's Mercy Health System*, JVR No. 1310080015, 2012 WL 9321069 (Mo.Cir.); *Parrott v. Williams, M.D.*, JVR No. 488364, 2006 WL 6012994 (S.C.); *Winkfield v. Mt. Carmel Health*, 2011 WL 2435471 (Ohio Com.Pl.); *Gomcsak v. Kovach, M.D.*, JVR No. 458584, 2004 WL 5279691 (Ohio); *Plaintiff v. Medlantic Healthcare Group Inc. D/B/A Washington Hospital Center*, JVR No. 395272, 1999 WL 34978669 (D.C.).

[18]*Peed v. Dimensions Healthcare Assocs.*, 2010 WL 7633919(Md.Cir.Ct.).

[19]21 N.E.3d 99 (Ind. Ct. App. 2014).

[20]U.S. Department of Health & Human Services. (n.d.) *Health information privacy.* www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities.

[21]N.J.A.C. 13:39-7.19; N.J.A.C. 13:39-9.19.

[22]*Cf.,* Jackson, J.Z. (2015, May 18) *The spectre of strict liability for an employee's HIPAA breach.* http://healthcareblog.mdmc-law.com.

[23]25 N.E.3d 748 (Ind. Ct. App.), *transfer denied,* 2015 Ind.LEXIS 374 (Ind. 2015).

[24]*See, e.g., Delaware Ins. Guaranty Ass'n v. Birch,* 2004 Del. Super. LEXIS 251, 2004 WL 1731139(Del. Sup. Ct. 2004).

[25]*See, e.g., Princeton Ins. Co. v. Chunmuang,* 151 N.J. 80, 98-99 (1997).

[26]*Cf., Harleysville Ins. Co. v. Garitta,* 170 N.J. 223, 231 (2001); *Hampton Medical Group, P.A. v. Princeton Ins. Co.,* 366 N.J. Super. 165, 173 (App. Div. 2004).

[27]45 CFR §164.401 (definitions of "breach" and "unsecured"); and 45 CFR §164.304 (definition of encryption).