The Metropolitan
Corporate Counsel®
National Edition
www.metrocorpcounsel.com
Volume 21, No. 12 December 2013

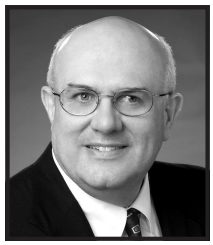
The Cost Of A Data Breach: The Health Care Perspective

Luis J. Diaz
David N. Crapo

Gibbons P.C.

The best-known provision of the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH") was the amendment of the Health Insurance Portability and Accountability Act of 1996 to provide for the promulgation by the U.S. Department of Health and Human Services ("HHS") of the Breach Notification Rule. An Interim Final Breach Notification Rule ("Interim Final Rule") was published on September 23, 2009. The Interim Final Rule generated significant controversy. On January 25, 2013, HHS issued the HIPAA Privacy, Security and Breach Notification: Final Omnibus Rule ("Omnibus Rule") which included a modified, and final, HIPAA Breach Notification Rule. 78 F.R. 5566, *et seq*. Much has been written on what constitutes a breach and how to prevent breaches. HHS estimates that as many as 700,000 entities will be subject to the Final Breach Notification Rule. 75 F.R. at 5671. This article will address an equally important issue, the cost of a breach, including (i) the cost of notifying individuals, HHS and media of a breach; (ii) civil monetary penalties that HHS can impose; and (iii) civil judgments.

Luis J. Diaz



David N. Crapo

1. The Cost Of Notification

The Breach Notification Requires mandates that affected individuals be notified of any breach of their protected health information ("PHI"). 45 C.F.R. § 164.404. A breach involving the PHI of more than 500 individuals must be reported to HHS (45 C.F.R. § 408) and, if the breach involves the PHI of more than 500 individuals in a single state or similar jurisdiction, the media. 45 C.F.R. § 164.406. A breach is the unauthorized access, acquisition, use or disclosure of PHI that compromises the PHI. 45 C.F.R. § 164.402.

HHS included an estimate of the costs of compliance with the Breach Notification Rule in the preamble to the Interim Rule. Three years later, armed with the statistics from two full years of reporting under the Breach Notification Rule, HHS included in the preamble to the Omnibus Rule a summary indicating that breach notification compliance costs totaled $14,475,600. 75 F.R. at 5670-5675. Those costs include the following: (i) E-mail and First Class Mail ($3,467,122); (ii) Substitute Notices: Media Notice ($571,200); (iii) Substituted Notices: Toll-Free Number ($1,816,379); (iv) Imputed cost to affected individuals who call the toll-free line ($2,042,665); (v) Notice to Media of Breach: Over 500 ($15,420); (vi) Report to HHS: 500 or More ($15,420); (vii) Investigation Costs: Under 500 ($5,277,456); (viii) Investigation Costs: 500 or More ($837,500); and (ix) Annual Report to the Secretary ($422,438). 75 F.R. at 5671. Consequently, compliance with the notification requirements of the Breach Notification Rule can be expensive, particularly if the number of individuals whose PHI has been compromised is large.

2. Civil Monetary Penalties

In addition to incurring expenses in notifying affected individuals, HHS and the media of a breach, the entity responsible for a breach may be subject to significant civil monetary penalties. Long viewed as a toothless tiger, HIPAA is now being enforced more vigorously. HITECH and the Omnibus Rule substantially increase the penalties for HIPAA violations – including those resulting in a breach of PHI. Under 45 C.F.R. § 160.404(b)(2), the penalties have been tiered based on culpability as follows:

- The entity did not know and could not have known of the HIPAA violation: Not less than $100 nor more than $50,000 per violation.
- There was reasonable cause for the HIPAA violation: Not less than $1,000 nor more than $50,000 for each violation.
- The HIPAA violation resulted from willful neglect on the part of the culpable entity but was corrected within 30 days of the date the entity became or should have become aware of the violation: Not less than $10,000 nor more than $50,000 per violation.
- The HIPAA violation resulted from

Luis J. Diaz *is a Director in the Intellectual Property Department of Gibbons P.C. in Newark, NJ and serves as the firm's Chief Diversity Officer. He focuses much of his practice on data privacy and security issues.* ***David N. Crapo*** *is Counsel in the Gibbons Financial Restructuring & Creditors' Rights Department and a member of the firm's Health Care Team. He focuses much of his health care practice on privacy and security issues.*

Please email the authors at ldiaz@gibbonslaw.com or dcrapo@gibbonslaw.com with questions about this article.

willful neglect and violation was not corrected: Not less than $50,000 per violation.

The penalty is capped at $1,500,000 for identical violations during a calendar year. *Id.*

Affinity Health Plan, Inc. ("Affinity") learned a hard lesson about HIPAA's enhanced penalties. Affinity returned a number of photocopiers to leasing agents without erasing PHI from their hard drives. As a result, the PHI of up to 344,579 individuals was compromised. Affinity notified HHS of the breach on April 15, 2010. HHS investigated the breach and determined that Affinity had failed to assess the potential security risks to PHI stored on photocopier hard drives and failed to implement policies for the removal of the PHI on those hard drives when the copiers were returned to leasing agents.

Affinity and HHS entered into a Resolution Agreement pursuant to which Affinity paid a penalty of $1,215,780 (which was in addition to the costs it had incurred in notifying affected individuals of the breach) and entered into a Corrective Action Plan ("CAP") with HHS. The CAP will result in still more breach-related expense to Affinity. Affinity must use its best efforts to retrieve the photocopier hard drives containing PHI and certify that it has done so. To the extent that Affinity is unable to retrieve all of the hard drives, it must provide HHS with documentation of the efforts it made to do so. Additionally, Affinity must conduct a HIPAA Security Rule risk analysis and develop a plan to mitigate any security risks and vulnerabilities that will be subject to review, comment and revision by HHS.

Hospice of North Idaho ("HNI") learned that the enhanced HIPAA penalties apply to small breaches and not just large ones. A laptop containing unencrypted PHI concerning 441 patients was stolen from HNI. HNI was assessed a $50,000 penalty. This was the first penalty assessed in connection with a breach affecting fewer than 500 people.

3. Litigation

Neither HIPAA, HITECH nor the Omnibus Rule provide a private cause of action. However, that has not stopped creative plaintiff's counsel from bringing litigation (including putative class actions) arising out of HIPAA violations.

On July 26, 2013, an Indiana jury awarded $1,440,000 to a Walgreen's customer whose PHI had been improperly accessed by a Walgreen's pharmacist. The pharmacist provided the PHI to her husband, the customer's former boyfriend. The customer sued Walgreen's asserting claims under Indiana law for negligent training and supervision of the pharmacist. The customer also sued the pharmacist asserting under Indiana law for breach of privacy. Walgreens plans to appeal the verdict. Nevertheless, the case presents an example of how private actions can be grounded in *intentional* violations of HIPAA.

Advocate Health and Hospital Corp. ("Advocate") of Downers Grove, Illinois is facing suits brought by three creative plaintiff's counsel. Apparently, Advocate has a policy of encrypting PHI, including PHI on laptops. However, the PHI housed in four laptops at an Advocate's premises was not encrypted when they were stolen on July 15, 2013. The PHI of more than 4 million individuals was compromised. Notification of affected individuals has begun, and HHS and the media have been notified of the breach.

Additionally, three class action complaints have been filed against Advocate: one in the United States District Court for the Northern District of Illinois and two in the Circuit Court of Cook County. The federal complaint, in *Erica Tierney et al., v. Advocate Health and Hospitals Corp et al*. (Civil Action No. 13-06237) asserts claims for (i) willful violations of the Fair Credit Reporting Act; (ii) negligent violation of the Fair Credit Reporting Act; (iii) negligence; and (iv) invasion of privacy by public disclosure of private facts. In one of the Cook County actions, *Alex Lozada, et al., v. Advocate Health and Hospitals Corporation, et al.* (Case No. 13-CH-20390), the named plaintiff asserts claims for (i) breach of contract (with Advocate's Notice of Privacy Practices constituting the contract); (ii) breach of implied contract; (iii) unjust enrichment (the breach demonstrates that the services the named plaintiff received were not worth what he paid for them); and (iv) breach of fiduciary duty. In the other Cook County action, *Pierre Petrich, et al. v. Advocate Health and Hospitals Corporation, et al*. (Case No. 13-L-009984), the named plaintiffs assert claims for (i) negligence; (ii) violation of the Illinois Consumer Fraud and Deceptive Business Practices Act; (iii) invasion of privacy; (iv) intentional infliction of emotional distress; and (v) violation of the Illinois Consumer Fraud Act.

Advocate has begun to seek dismissal of the class actions. Advocate will likely argue that: (i) the statutes on which the plaintiffs rely are not applicable; (ii) the plaintiffs' allegations are insufficient to support a claim for any intentional tort; and (iii) its Notice of Privacy Practices does not constitute either an express or implied contract. Advocate has also begun to challenge class certification. Thus, Advocate is now incurring the expense of challenging class certification and dispositive motions. Additionally, to the extent that some of the claims survive dispositive motions and a class is not certified, there will certainly be the expense of multiple litigation.

4. Additional Costs

Data privacy and security breaches involve hidden costs that cannot easily be quantified if at all. The first cost is reputational damage. In that regard, HHS is required to, and does, publish a list of breaches affecting more than 500 individuals on its website. *See http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.* Larger breaches draw unfavorable media attention. Entities responding to a breach suffer productivity loss due to employee time and effort involved in the breach investigation and responding to patient inquiries about the breach. Those entities also may have to incur the cost of providing credit monitoring services to affected individuals, particularly if there is any indication that the unauthorized party who has accessed or acquired PHI or to whom it has been disclosed is part of an identity theft ring. Finally, a large breach erodes patient and public trust.

5. Conclusion

As demonstrated above, the costs (both calculable and non-calculable) arising from a data security or privacy breach are reason enough for entities covered by HIPAA to have robust privacy and security policies and procedures in place.