Litigation in a HITECH World

Cybersecurity and the Importance of Maintaining HIPAA Security Compliance

By Aaron P. Sohaski and Jordan B. Segal

Attorneys who represent healthcare providers or others in the healthcare industry must be well-versed in the Health Insurance Privacy and Accountability Act (HIPAA) Privacy Rule. Litigators, in particular, must have a working knowledge of the rule to prevent inadvertent disclosures of protected personal health information during discovery. But HIPAA also has a set of rules that require sophisticated cybersecurity protocols.

How important is cybersecurity to healthcare clients? According to a survey of both in-house healthcare compliance officers and outside consultants compiled by the Society of Corporate Compliance and Ethics and the Health Care Compliance Association, it is the highest-ranked hot topic for 2016.[1] A recent wave of so-called "ransomware" attacks that targeted hospitals may have brought cybersecurity to the forefront.[2] Regardless of the cause, attorneys representing clients in the healthcare field must now be equally well-versed in cybersecurity—not merely because it is a concern for clients, but also because practicing law in this arena carries real risks of regulatory action.

Attorney liability under HIPAA

HIPAA was passed in 1996 to ensure that patients' health records remain confidential.[3] The act requires that any party—physician or other healthcare provider or their business associates (entities that provide support to healthcare practices by providing services such as accounting, administration, or legal representation and may come into contact with protected patient information[4])—must ensure the safety of patient information both inside and outside of the healthcare facility. In 2009, Congress gave HIPAA some regulatory teeth by passing the Health Information Technology for Economic and Clinical Health Act (HITECH) as part of the American Recovery and Reinvestment Act. HITECH included several provisions to address privacy and security concerns associated with the electronic transmission of health information and added several provisions to strengthen the civil and criminal enforcement of HIPAA rules. As amended by HITECH, HIPAA also requires Internet service providers to maintain the integrity of health records, illustrating the seriousness of the government's concerns with privacy and security policy.

Post-HITECH, litigators must be vigilant to maintain HIPAA compliance, as failure to observe the act's requirements can have dire consequences for both litigators and their clients. While HIPAA's Security Rule has not yet been the basis for penalties against a law firm, it may only be a matter of time given recently increased scrutiny and oversight by regulators. Thus, law firms—particularly those litigating matters that require discovery of HIPAA-protected materials—should be proactive in protecting themselves from HIPAA Privacy Rule and Security Rule violations.

For example, in the 2004 case *Law v Zuckerman*,[5] the federal district court for the District of Maryland examined whether the unauthorized release of patient information to defense counsel in a medical malpractice suit violated HIPAA. The court found a HIPAA violation, stating, "To the extent there was a disclosure of individually identifiable health information, Defendant's pretrial contacts with [the doctor] were in violation of HIPAA."[6] The court concluded, however, that sanctions were not appropriate under the circumstances of that case. Other attorneys have not been so fortunate.[7] To be sure, HIPAA does not *preclude* the disclosure of personal health information during discovery, but it requires a specific procedure—including the use of "qualified protective orders"—when doing so.

A qualified protective order must satisfy several requirements. First, it must prohibit defendants from disclosing the plaintiff's protected information outside the scope of the litigation.[8] Second, the order must require that defendants return or destroy the protected information when litigation concludes.[9] Third, although not explicitly required by HIPAA's Privacy Rule, some courts have also required that, if the protective

A recent wave of so-called "ransomware" attacks that targeted hospitals may have brought cybersecurity to the forefront.

"Trial Practice" is a regular column of the *Michigan Bar Journal*, edited by Gerard Mantese and Theresamarie Mantese for the Publications and Website Advisory Committee. To contribute an article, contact Mr. Mantese at gmantese@manteselaw.com.

Post-HITECH, litigators must be vigilant to maintain HIPAA compliance, as failure to observe the act's requirements can have dire consequences for both litigators and their clients.

order permits defense counsel to seek an ex parte interview with a litigant's physician, it must contain "clear and explicit" notice to the physician about the purpose of the interview and that the physician is not required to speak to counsel.[10] Qualified protective orders have become so commonplace that many courts have developed standardized form orders for use by litigants.

HIPAA's Security Rule

Since the passage of HIPAA and its modification under HITECH, most lawyers have become familiar with these policies and the necessary practices to avoid liability under HIPAA's Privacy Rule. Consequently, attorney liability under the rule is rare. However, HIPAA also contains a second set of regulations collectively referred to as the Security Rule,[11] which can assess liability for failing to adequately protect personal health information, even when it has been properly disclosed.

Specifically, the Security Rule requires that covered entities and business associates (which can include law firms[12]):

(1) ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

(2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

(3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

(4) ensure compliance by its workforce.[13]

The Federal Trade Commission's recent action in *In re Henry Schein Practice Solutions, Incorporated*[14] illustrates the increasing scrutiny of cybersecurity practices under the Security Rule. Henry Schein Practice Solutions, Inc. (Henry Schein) owns and licenses the use of Dentrix software, which enables dentists to perform common office tasks including entering patient data, sending appointment reminders, and processing payments in a web-based portal.[15] In 2012, Henry Schein introduced Dentrix with a new database engine provided by a third party.[16] The company advertised this software as carrying "industry standard" encryption to its dentists, and dentists used it to collect and store patients' personal information.[17] However, as far back as November 2010, the database engine vendor informed Henry Schein that the algorithm protecting patient records had not been tested publicly and was not industry-standard encryption protocol.[18]

The Federal Trade Commission claimed that Henry Schein's misleading advertisement about its security protocols was an unfair or deceptive practice and that the company failed to satisfy its regulatory obligations under the Security Rule. Henry Schein and the FTC quickly entered into a consent order under which the company was required to pay $250,000. Additionally, Henry Schein agreed it will no longer state that its product uses industry-standard encryption and ensures compliance with the Security Rule. Moreover, the company was required to notify all customers who purchased Dentrix G5 of the misleading statements.

While Henry Schein is not a law firm, this case serves as a cautionary tale. Any law firm that represents healthcare clients may well be considered a business associate to whom the Security Rule applies.[19] For example, both a creditor's rights firm seeking to collect debts on behalf of a hospital and an employment firm providing legal advice to a hospital on hiring practices could be considered business associates.[20] Pursuant to HITECH's amendments, all business associates must observe the technical and technological requirements of the Security Rule.[21]

Requirements of HIPAA's Security Rule

In contrast to the specific requirements of HIPAA's Privacy Rule, the Security Rule is much more flexible and leaves the burden of designing cybersecurity protocols to each individually covered entity or business associate.[22] Although not specifically stated in the rule, data is typically considered secured if the personal health information is encrypted and protected according to National Institute of Standards and Technology guidelines.[23] More specifically, the Security Rule enumerates five types of safeguards that a personal health information data security plan should cover.

Administrative safeguards[24]

The administrative safeguards section requires that covered entities or business associates "[i]mplement policies and procedures to prevent, detect, contain, and correct security violations."[25] This section contains more than half of the Security Rule's specific requirements, which include that the covered entity or business associate (1) perform a risk analysis of its data security, (2) implement a risk management program to "reduce risks and vulnerabilities to a reasonable and appropriate level,"[26] (3) create a policy outlining sanctions for employees and vendors who fail to comply with the risk management and data security policy,[27] and (4) regularly review data logs and information system activities for potential breaches.[28]

Physical safeguards[29]

Physical safeguards are the physical measures that need to be put in place to ensure that the working environment is HIPAA-compliant and information is kept safe. These safeguards include limited facility and access control with authorized access in place. They also include a requirement to maintain policies and procedures

regarding the transfer, removal, disposal, and reuse of electronic media to ensure appropriate protection of electronic personal health information.

Technical safeguards[30]

These safeguards are generally aimed at electronic security measures that are implemented in the healthcare system. Technical safeguards can include access control measures such as unique user IDs (fingerprint scanning, voice control, eye scanners, or ID cards), emergency access procedures, and automated log off on all computers and electronic devices as well as encryption and decryption methods. They also include measures that limit the electronic distribution of sensitive patient information. Every healthcare provider is required to sign up with a HIPAA-compliant host to ensure that electronic communication is secure. This host acts as a first line of defense against any illegal access of content contained in electronic communication. It also covers the safety measures of all electronic systems—e-mails, private networks, and private web-based or cloud-based systems and software.

Organizational requirements[31]

The organizational requirements ensure that relationships between covered entities and business associates or between business associates and their vendors and subcontractors include compliance with HIPAA's Security and Privacy rules. The Department of Health and Human Services has published a form business associate agreement.[32] The organizational requirements also include a duty—if a covered entity or business associate learns of a breach of the agreement or of the Privacy Rule or Security Rule—to terminate the contract or arrangement if feasible or, if termination is not feasible, report the breach to authorities.

Policies and procedures and documentation requirements[33]

Written policies and procedures should align with the technical safeguards. These policies should also cover integrity controls that have been put in place to prevent electronic protected health information from being destroyed or leaked. It should reflect the information technology disaster recovery process, including an off-site or remote backup. This will help staff in illustrating what should be done to remedy electronic media errors and failures. The backup should also be able to recover sensitive patient information and restore it without any discrepancies or damage to the integrity of the data.

Conclusion

While the concept of data privacy under HIPAA's Privacy Rule has been quickly adopted and understood by litigators, data security and cybersecurity are often overlooked by litigators who may or may not be technologically savvy. These litigators understand and have developed practices to avoid liability for violations of the Privacy Rule. However, as data and cybersecurity become increasingly important to the healthcare industry, litigators must also develop a similar familiarity with HIPAA and HITECH security rules. ■

Aaron P. Sohaski is a licensed attorney who works for the Henry Ford Health System in Detroit, handling contract compliance. A recent graduate of Western Michigan University Cooley Law School, he served as the 6th Circuit governor and national chair within the ABA Law Student Division. Currently, he serves on the SBM Young Lawyers Section Council and is active in local bar associations.

Jordan B. Segal is an associate at the firm of Mantese Honigman, PC, in Troy where he practices business, employment, and healthcare litigation.

ENDNOTES

1. Society of Corporate Compliance and Ethics and the Health Care Compliance Association, *Compliance and Ethics Hot Topics for 2016* (January 2016) <http://www.corporatecompliance.org/Portals/1/PDF/Resources/Surveys/2016-hot-topics-survey-report.pdf?ver=2016-02-15-092521-740>. All websites cited in this article were accessed October 20, 2016.
2. Gallagher, *Two more healthcare networks caught up in outbreak of hospital ransomware* (March 29, 2016) <http://arstechnica.com/security/2016/03/two-more-healthcare-networks-caught-up-in-outbreak-of-hospital-ransomware>.
3. PL 104-191; 110 Stat 1936.
4. 45 CFR 160.103.
5. *Law v Zuckerman*, 307 F Supp 2d 705 (D Md, 2004).
6. *Id.* at 711.
7. E.g., *Parker v Upsher-Smith Labs, Inc*, unpublished order of the US District Court for the District of Nevada, entered February 18, 2009 (Docket No. 06-0518) (issuing sanctions because plaintiff's counsel impermissibly contacted the decedent's treating physicians).
8. 45 CFR 164.512(e)(1)(v)(A).
9. 45 CFR 164.512(e)(1)(v)(B).
10. *Palazzolo v Mann*, unpublished opinion of the US District Court for the Eastern District of Michigan, issued March 19, 2009 (Docket No. 09-10043), p 4; *Harhara v Norville*, unpublished order of the US District Court for the Eastern District of Michigan, issued September 18, 2007 (Docket No. 07-12650), p 4.
11. Codified at 45 CFR Parts 160, 162, and 164.
12. See Bradshaw & Hoover, *Not So Hip?: The Expanded Burdens on and Consequences to Law Firms as Business Associates under HITECH Modifications to HIPAA*, 13 Rich J L & Pub Int 313 (2010).
13. 45 CFR 164.306(a)(1–4).
14. *In Re Henry Schein Practice Solutions, Inc*, unpublished decision and order of the Federal Trade Commission, issued May 20, 2016 (Docket No. C-4575).
15. *Id.*
16. *Id.*
17. *Id.*
18. *Id.*
19. See *Graham v Fleissner Law Firm*, unpublished order of the US District Court for the Eastern District of Tennessee, issued May 22, 2008 (Docket No. 1:08-cv-00031), p 3 (noting that only those law firms who are not representing covered entities are not regulated under HIPAA).
20. *Not So Hip?*, 13 Rich J L & Pub Int 313.
21. 42 USC 17931(a); 45 CFR 164.308, 164.310, and 164.312.
22. See 42 CFR 164.306(b)(1) ("Covered entities and Business Associates may use *any security measures* that allow the covered entity or Business Associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.") (Emphasis added.)
23. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (February 12, 2014) <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>.
24. 42 CFR 164.308.
25. 42 CFR 164.308(a)(1)(i).
26. 42 CFR 164.308(a)(1)(ii)(B).
27. 42 CFR 164.308(a)(1)(ii)(C).
28. 42 CFR 164.308(a)(1)(ii)(D).
29. 42 CFR 164.310.
30. 42 CFR 164.312.
31. 42 CFR 164.314.
32. Available online at <http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>.
33. 42 CFR 164.316.