Bloomberg BNA

Health IT Law & Industry Report™

VOL. 8, NO. 11 MARCH 14, 2016

BNA INSIGHTS

HIPAA Data Storage Considerations to Protect Patient Records

BY RICHARD A. BLUNK AND LORINDA HARRIS

Richard A. Blunk is managing director and general counsel of Thermopylae Ventures, LLC, a Dallas-based alternative investment group with interests in cyber security, intellectual property monetization, alternative litigation finance, fire retardants, Internet addresses, inbound foreign investment, vocational rehabilitation equipment and Texas real estate. He can be reached at rblunk@thermopylaeventures.com.

Lorinda Harris is of counsel at DLA Piper in Sacramento, Calif. She counsels clients on data privacy and security regulatory compliance, primarily in the health-care industry. She can be reached at lorinda.harris@dlapiper.com

Cyber attacks and their associated costs are on the rise, as underscored in the recent extortion of Hollywood Presbyterian by hackers that infected the hospital's computer system with ''ransomware''—a malicious software program that locks down computer networks and holds them for ransom.

The hospital paid $17,000 in Bitcoin to regain access to its patients' health records.[1]

The United States Department of Health and Human Services Office for Civil Rights (OCR) has also stepped up its enforcement activities, issuing its second civil monetary penalty for violations of the Health Insurance Portability and Accountability Act of 1996; this time against a home health care agency.[2] OCR's largest

[1] *Cybersecurity Firms: Ransomware a Growing Problem for Hospitals*, HEALTH IT LAW & INDUSTRY REPORT, Feb. 29, 2016 (*see previous story*)

[2] *Civil Fine Against Lincare Upheld for HIPAA Violation*, BNA's HEALTH CARE DAILY REPORT, Feb. 5, 2016.

 ISSN 2151-2876

settlement of $4.8 million with New York Presbyterian Hospital and Columbia University Medical Center followed a physician's attempt to deactivate a personally owned computer server on the network, resulting in the exposure of 6,800 patient records.[3]

More recently, OCR settled with the University of Washington for $750,000 when approximately 90,000 individuals' electronic protected health information (ePHI) was accessed after an employee downloaded an email attachment containing malicious software.[4]

Given this troubling trend, it is reasonable to expect that the true cost of health care breaches will continue to be substantial,[5] including not just settlements and penalties but also negative brand perception and reputation loss, business interruption, loss of intellectual property, regulatory action, system repair and data loss, personal injury and property damage, breach of contract, director's liability, fraud, and ransom payments.

It is reasonable to expect that the true cost of health care breaches will continue to be substantial.

HIPAA sets forth the first set of national standards for the protection of health care information including ePHI.[6] The HIPAA Privacy Rule recognizes the need to ''assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being.''[7]

To reach this laudable goal, entities (both Covered Entities and Business Associates following passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, jointly, with the 1996 law, HIPAA)[8] must maintain ''reasonable and appropriate'' safeguards to prevent the improper or unauthorized use or disclosure of ePHI.[9]

The HIPAA Security Rule[10] establishes national standards to protect individuals' ePHI by requiring appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of ePHI based upon a risk analysis and management framework, as well as organizational, policy, procedural and documentation requirements.[11]

The Security Rule classifies ''required'' and ''addressable'' standards.[12] ''Required'' specifications include employee sanctions' policies, written contracts with Business Associates (''Business Associate Agreements''), unique user identification protocols, emergency access procedures, information system activity review, ePHI disposal, security incident response procedures, and contingency planning.[13]

Entities should be in good stead as long as appropriate security measures are employed to achieve the goal of protecting against reasonably foreseeable cyber threats.

While the Security Rule's ''required'' provisions must certainly be followed, even these parameters come with flexibility and discretion. The Security Rule is ''techno-

[3] U.S. Dep't of Health & Human Services, Office for Civil Rights, Data Breach Results in $4.8 Million HIPAA Settlements, *available at* http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/new-york-and-Presbyterian-hospital/index.html. *See also U.S. Dep't of Health & Human Services*, Office for Civil Rights, Summary of the HIPAA Privacy Rule 3-4, *available at* http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations (hereinafter *Summary of HIPAA Privacy Rule*).

[4] U.S. Dep't of Health & Human Services, Office for Civil Rights, $750,000 HIPAA settlement underscores the need for organization-wide risk analysis (Dec. 14, 2015), *available at* http://www.hhs.gov/about/news/2015/12/14/750000-hipaa-settlement-underscores-need-for-organization-wide-risk-analysis.html.

[5] *Community Health Systems breach cost estimates as high as $150 million*, FierceHealthIT (Aug. 25, 2014) http://www.fiercehealthit.com/story/community-health-systems-breach-cost-estimated-75m-150m/2014-08-25.

[6] *Summary of HIPAA Privacy Rule* at 1. The Privacy Rule, adopted as ''Standards for Privacy of Individually Identifiable Health Information,'' is available at http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/introduction/index.html.

[7] *Summary of HIPAA Privacy Rule* at 1.

[8] The term ''covered entities'' includes health plans, health care providers, health care clearinghouses and their respective business associates, which includes entities such as cloud computing providers and entities that perform on-site data aggregation and analysis. *Id.* at 2.

[9] *Id.* at 14.

[10] U.S. Dep't of Health & Human Services, Office for Civil Rights, Summary of the HIPAA Security Rule, *available at* http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations (hereinafter *Summary of HIPAA Security Rule*). The HIPAA Security Rule is codified in 45 C.F.R. Part 160 and Subparts A and C of Part 164.

[11] *See generally* Matthew Scholl et al., *An Introductory Resource Guide for Implementing Health Insurance Portability and Accounting Act (HIPAA) Security Rule*, U.S. Dep't of Commerce, National Institute of Standards and Technology, at 7-8, *available at* http://www.nist.gov/manuscript-publication-search.cfm?pub_id=890098 (hereinafter *NIST Framework*).

[12] *Summary of HIPAA Security Rule* at ''Required and Addressable Implementation Specifications.''

[13] *Security Standards: Physical Safeguards*, HIPAA Security Series 3, Dep't of Health & Human Services, Center for Medicare & Medicaid, at 15 (Mar. 2007), *available at* http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf. (hereinafter *Physical Safeguards*); *Security Standards: Technical Safeguards*, HIPAA Security Series 4, Center for Medicare & Medicaid, Dep't of Health & Human Services, Mar. 2007, at 16, *available at* http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf (hereinafter *Technical Standards*); *Security Standards: Organizational, Policies and Procedures and Documentation Requirements*, HIPAA Security Series 5, Center for Medicare & Medicaid, Dep't of Health & Human Services, Mar. 2007, at 16, *available at* http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/pprequirements.pdf (hereinafter *Organizational Standards*).

  HITR ISSN 2151-2876

logically neutral,'' meaning it does not mandate the use of specific technologies.[14]

Rather, entities should be in good stead as long as appropriate security measures are employed to achieve the goal of protecting against reasonably foreseeable cyber threats.[15]

Determining what is reasonable and appropriate requires a thoughtful consideration of factors ranging from the size, complexity and capabilities of the organization, technical infrastructure, hardware and software capabilities, the cost of security precautions, the scope and type of ePHI at issue, and the potential magnitude and probability of risks associated with an impermissible use or disclosure of ePHI.[16]

This analysis must be ongoing and evolve in the face of changing technologies and cyber threats.[17]

''Addressable'' standards, while not mandatory, are nonetheless Security Rule guidelines to be followed when reasonable and appropriate.[18] Addressable criteria range from aspects of Workforce authorization, supervision, clearance and termination procedures, access authorization, access establishment and modification, security reminders, protection from malicious software, log-in monitoring, password management, testing and revision procedure, access control and validation procedures, data backup and storage, automatic logoff, and transmission security.[19]

In sum, HIPAA-regulated entities must have cyber security programs that protect against ''reasonably anticipated threats to the security or integrity'' of ePHI.[20] Such programs must implement, maintain and update the selected cyber security measures.[21]

Presently, with the narrow exception of full encryption of data at rest and in transit, there is not a robust ''safe harbor'' whereby a ''reasonable'' cyber security program constitutes automatic compliance.[22] In the absence of a vigorous safe harbor, reasonableness imbues the compliance process with a degree of elasticity and flexibility appropriate to evolving technologies and accompanying threats.

Analysis of reasonable and appropriate measures must be ongoing and evolve in the face of changing technologies and cyber threats.

Case law provides some direction.[23] The language in several recent decisions has suggested that the Security Rule can serve as a standard of care in private negligence suits brought by individuals alleging a HIPAA breach.[24] As HIPAA does not provide for private rights of action, this trend toward private rights of action could raise entities' exposure.[25]

For a useful resource in determining what constitutes a reasonable security program, many turn to the National Institute of Standards and Technology (''NIST'').[26] NIST offers administrative, physical, technical and organizational safeguards, as well as suggested policies and procedures.[27]

While implementing these NIST safeguards is voluntary, NIST suggests that ''. . .private sector organizations composing the critical health infrastructure of the United States are encouraged to consider using these guidelines, as appropriate.''[28] NIST's framework is designed for a variety of industries, not just healthcare,[29] and is useful in identifying security weaknesses and setting security goals for all types of companies.[30]

Turning now to how to store your protected health information, entities have several options involving distinct considerations. Historically, such data has been managed on-site. Yet in recent years HIPAA-regulated entities have increasingly turned to Cloud providers for data storage.

Cloud advocates cite lower costs, rapid and smart scalability of resources, and timely, effective and efficient security measures.[31]

---

[14] *Summary of HIPAA Security Rule* at ''General Rules.''

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Summary of HIPAA Security Rule* at ''Required and Addressable Implementation Specifications.''

[19] *Physical Standards* at 16; *Technical Standards* at 15-17; *Organizational Standards* at 11.

[20] *Summary of HIPAA Security Rule* at ''General Rules.''

[21] *See Summary of HIPAA Privacy Rule & Summary of HIPAA Security Rule*.

[22] *See Dep't of Health & Human Services, Office for Civil Rights, Guidance on Risk Analysis Requirements under the HIPAA Security Rule*, at 4 (July 14, 2010), *available at* http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf (hereinafter *Guidance on Risk Analysis*).

[23] *See generally Reasonable Security Program*.

[24] *Can A HIPAA Violation Give Rise to a Private Cause of Action?*, Dallas/Fort Worth Healthcare Daily (May 27, 2014), http://healthcare.dmagazine.com/2014/05/27/can-a-hipaa-violation-give-rise-to-a-private-cause-of- action.

[25] *Id*.

[26] Peter Sloan, *The Reasonable Information Security Program*, 21. Rich. J.L. & Tech. 2, 28 (2014), *available at* http://jolt.richmond.edu/v21i1/article2.pdf (hereinafter *Reasonable Security Program*).

[27] *See generally NIST Framework*.

[28] *Id.* at 3.

[29] *See* Scott Shackleford et al., *Toward a Global Cybersecurity Standard of Care?*, 50 Tex. Int'l L.J. 305, 327-28 (2015).

[30] *See id.* at 331-32.

[31] European Network &Information Security Agency, Cloud Computing—Benefits, risks and recommendations (Dec. 2012) at 5-6, *available at* https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security (hereinafter *Revised ENISA Report*).

Cloud storage has these and other benefits, but its use also raises questions of control.

Entities that store data in the Cloud cede physical control over its data to the Cloud provider, shifting some of the burden—but not necessarily the responsibility or liability—to the provider to protect against breaches. And depending upon where the data is stored, Cloud storage may also subject entities to extraterritorial laws and regulations.[32] The Cloud's economics of scale and flexibility are both a friend and a foe from a security point of view.[33]

The Cloud's economics of scale and flexibility are both a friend and a foe from a security point of view.

Entities opting for Cloud storage should—and frequently can—proactively minimize potential risks. Entities must carefully vet Cloud providers; merely turning over ePHI—even to a ''HIPAA-compliant'' Cloud provider—does not relieve a HIPAA-regulated entity of its own HIPAA obligations.[34] In vetting Cloud providers, entities should question and become comfortable with the provider's data segregation methods, breach and security incident protocols, back up or emergency measures, and general security safeguards.

For guidance, entities may look to recent Federal Trade Commission (FTC) cases involving Cloud storage privacy breaches.[35] In one such case, *In re GMR Transcription Services, Inc.*, the FTC concluded that a medical transcription services company engaged in an unfair and deceptive trade practice by failing to adequately select, contract with, and oversee its Cloud provider.[36]

According to the FTC, the transcription services company failed to require the Cloud provider ''to adopt and implement appropriate security measures'' or to ''take adequate measures to monitor and assess whether [the Cloud provider] employed measures to appropriately protect personal information under the circumstances.''[37] Commentators have observed that the case ''solidifies the principle that companies have duties of data service provider management in choosing, contracting with and overseeing vendors,''[38] which the FTC now seems to have extended to Cloud storage providers.[39]

Risks unique to Cloud storage include data comingling, network breaks, congestion, misconnection and non-optional use, modification of network traffic, privilege escalation, interception of data in transit, data leakage on upload and/or download, possible deletion of metadata that may be relevant to future litigation, insecure or ineffective deletion of data, distributed denial of service, loss of encryption keys, social engineering, loss or compromise of operational and/or security logs, lost or stolen backups, unauthorized access to physical facilities, theft, hackers, and natural disasters.[40] These risks, however, may be minimized with proactive due diligence and oversight of Cloud providers.

Risks may be minimized with proactive due diligence and oversight of Cloud providers.

Still, entities should not overlook the relative benefits of federated, on-site storage since on-site storage may avoid the uncertainty of ceding control over ePHI to third parties. Plus, improving interoperability standards could potentially bring Cloud-like flexibility to on-site data systems like ''data lakes'' (a large storage repository and processing engine).[41]

Regardless of how data is stored, the Security Rule's ''reasonableness'' standard applies.[42] Risks exist with any data storage method. With proper vetting, Cloud storage is a practicable option.

Conclusion

Each entity must conduct its own risk assessment and due diligence in analyzing its data storage options, regardless of whether it moves its ePHI to the Cloud or maintains it on-site. Perhaps the absence of a robust HIPAA cyber security safe harbor should be viewed as positive; the flexibility afforded by the Security Rule allows entities to evolve with improvements in cyber security technology.[43] Since a ''reasonable'' cyber secu-

[32] *See Opinion 8/2014 on the Recent Developments on the Internet of Things*, THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, at 10 (Sept. 16, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

[33] *Revised ENISA Report* at 5.

[34] *See* Wayne Jansen & Timothy Grance, *Guidelines on Security and Privacy in Public Cloud Computing*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, at vi-vii (Jan. 2011), *available at* http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909494 (hereinafter *Guidance on Cloud Computing*).

[35] Daniel Solove & Woodrow Hartzog, *The FTC and Privacy and Security Duties for the Cloud*, BNA PRIVACY & SECURITY LAW REPORT, April 4, 2014, hereinafter *FTC and Cloud Security*).

[36] Complaint, *In re GMR Transcription Services, Inc.*, File No. 122 3095 (Jan. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140203gmrcmpt.pdf (hereinafter *GMR Complaint*); *see also* Complaint, *In the Matter of ASUSTeK Computer, Inc.* (Feb. 23, 2016) (alleging that a router manufacturer and Cloud provider engaged in an unfair act or practice by failing to secure private consumer information).

[37] *GMR Complaint* at 4.

[38] *FTC and Cloud Security* at 2.

[39] *See FTC and Cloud Security* at 2; *see also GMR Complaint* at 2 (describing the internet-based services provided by the transcription service provider).

[40] EUROPEAN NETWORK & INFORMATION SECURITY AGENCY, CLOUD COMPUTING – BENEFITS, RISKS AND RECOMMENDATIONS, at 47–52 (Nov. 2009), *available at* https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment (hereinafter *Initial ENISA Report*).

[41] *See generally Office of the National Coordinator for Health Information Technology*, 2015 INTEROPERABILITY STANDARDS ADVISORY, AVAILABLE AT https://www.healthit.gov/sites/default/files/2015interoperabilitystandardsadvisory01232015final_for_public_comment.pdf.

[42] *Summary of HIPAA Security Rule* at ''General Rules.''

[43] *See Summary of HIPAA Security Rule*.

  HITR ISSN 2151-2876

rity system must continue to adapt to a changing and increasingly more hostile risk matrix, entities should remain aware of the risks and returns of all available technologies in order to satisfy the evolving requirements of the HIPAA privacy and security regime.