Bloomberg BNA

BNA's
Health Law Reporter™

U.S. Privacy and Security Compliance Enforcement in the Health Care Industry: Recent Developments and Trends

BERNADETTE M. BROCCOLO AND EDWARD G. ZACHARIAS

Data breach has become one of the most challenging dimensions of enterprise risk management for health care organizations. Data breaches are an everyday occurrence and the subject of prominent and relentless media coverage. The struggle to keep pace with the ingenuity and aggressiveness of data breach perpetrators is daunting. Everyone is a target and a potential victim, including the federal government. Government agencies are stepping up enforcement with the Federal Trade Commission (FTC) playing a more active role, private parties are actively seeking redress in federal and state courts, and the U.S. Supreme Court has identified data privacy and security as an area deserving of its time and attention. Recent case law and government agency guidance are clearly influencing data security practices and patient and consumer expectations, but agency and court processes move slowly.

Remaining aware of these recent developments and trends is essential for any data security risk management endeavor. This article provides a review of such developments and trends and practical observations and insights for responding to them.

Bernadette M. Broccolo is a partner in McDermott Will & Emery's Chicago office who has practiced health law for over 35 years and focuses on privacy, information technology, clinical research program compliance, and corporate governance. She can be reached at bbroccolo@mwe.com.

Edward G. Zacharias is a partner in the firm's Boston office who provides regulatory and transactional representation to a range of health care organizations and services providers. He can be reached at ezacharias@mwe.com.

The authors acknowledge the substantial research and other contributions to this article by Ryan Marcus, a third year law student at Loyola University Chicago School of Law.

OCR's HIPAA Enforcement: Track Record and Current Enforcement Posture

Enforcement of the Health Insurance Portability and Accountability Act is a clear priority for the Health and Human Services Department's Office for Civil Rights. Shortly after being named OCR Director in June 2014, Jocelyn Samuels stated that ''enforcement is a critical part of [OCR's] arsenal of tools to ensure compliance,''[1] and that ''[OCR is] not in the business of certifying—like the *Good Housekeeping* seal.''[2]

Since 2009, 1,140 large health data breaches have been reported to OCR, involving more than 41 million people,[3] and in 2014 alone, OCR entered into more resolution agreements[4] and collected more in financial penalties than in any prior calendar year.[5] As of this

[1] Jocelyn Samuels, Director, Office for Civil Rights, HHS, Address at Conference on Safeguarding Health Information: Building Assurance through HIPAA Security (Sept. 23, 2014) (an annual HIPAA conference co-hosted by OCR and National institute of Standards and Technology).

[2] Dan Bowman, *Jocelyn Samuels: Privacy and Data Sharing Can Coexist, Fierce Health IT* (June 4, 2015), *available at* http://www.fiercehealthit.com/story/jocelyn-samuels-privacy-and-data-sharing-can-coexist/2015-06-04.

[3] Charles Ornstein, *Fines Remain Rare Even as Health Data Breaches Multiply*, PROPUBLICA (Feb. 27, 2015), *available at* http://www.propublica.org/article/fines-remain-rare-even-as-health-data-breaches-multiply#.

[4] Resolution agreements are OCR enforcement settlements that include a financial component and, typically, a corrective action plan.

[5] *See* U.S. Dep't of Health and Human Servs., *County Government Settles Potential HIPAA Violations*, *available at* http://www.hhs.gov/news/press/2014pres/03/20140307a.html (last updated Mar. 7, 2014) (reaching a settlement of $215,000 with the Skagit County Public Health Department after the acciden-

writing, however, OCR had entered into a total of only 24 resolution agreements for violations of the HIPAA privacy, security and breach notification standards over the course of its entire HIPAA enforcement history. OCR has announced only one resolution agreement in 2015.[6] Thus far, the agency has resolved most HIPAA violations by providing technical assistance, obtaining voluntary compliance or corrective action, and it has reserved resolution agreements ''to settle investigations with more serious outcomes,''[7] such as those involving ''systemic or long-standing concerns.''[8]

The impetus for OCR's new emphasis on its enforcement role may be any one or more of several factors: (1) the criticism of OCR's enforcement record by Congress[9] and more recently by the Office of Inspector General;[10] (2) increased financial resources to both support and incentivize increased OCR enforcement initiatives generated by the HITECH Act requirement that any civil monetary penalty or monetary settlement collected from a covered entity or business associate for a HIPAA violation must be transferred to OCR for use in enforcing HIPAA;[11] (3) an expectation that, with at least 10 years of compliance experience since the promulgation of the final Privacy Rule and the final Security Rule, covered entities should be expected to have an effective HIPAA compliance program; and (4) an increased volume or breach reports by covered entities resulting from the lower breach notification threshold adopted in the final HIPAA Omnibus Regulations that is now in effect. Regardless of the driving force, covered entities and business associates should expect and be prepared for continued, and perhaps more aggressive, and less sympathetic, supportive and collaborative OCR investigations and enforcement actions going forward.

In addition to enforcement activities generated by OCR investigations and compliance reviews occurring in response to breach reports and other ordinary course circumstances, enforcement actions also could result from a new round of HIPAA compliance audits OCR will initiate this year. The 2009 Health Information Technology for Economic and Clinical Health Act (HITECH Act) requires the U.S. Department of Health and Human Services (HHS) to conduct periodic audits to ensure covered entities and business associates are complying with the HIPAA privacy, security, and breach notification standards.[12] OCR conducted a first phase of periodic audits encompassing 115 covered entities in 2011 and 2012, and recently initiated a second round of audits by distributing pre-audit screening surveys requesting organizational and contact information. OCR has indicated that the surveys will be sent to covered entities from a pool of from 550 to 800 covered entities it identified through the National Provider Identifier database and other external sources. OCR plans to audit approximately 350 of the covered entities in this pool, including 232 health care providers, 109 health plans and 9 health care clearinghouses.[13] OCR will also audit select business associates from among those identified in the course of the covered entity audits.

OCR will use the findings from the second phase of audits to identify technical assistance it should develop for covered entities and business associates. A senior OCR official has warned, however, that, ''unlike the pilot audits, [these second phase audits] will be likely to result in compliance reviews'' and ''will be an enforcement tool.''[14]

---

tal placement of a file of receipts for medical services for 1,581 individuals on the internet); *see* U.S. Dep't of Health and Human Servs., *Data Breach Results in $4.8 Million HIPAA Settlements*, *available at* http://www.hhs.gov/news/press/2014pres/05/20140507b.html (last updated May 8, 2014) (reaching multimillion dollar settlements with Columbia University and New York and Presbyterian Hospital after a physician deactivated a personal server, accidentally disclosing PHI on the internet); *see* U.S. Dep't of Health and Human Servs., *$800,000 HIPAA Settlement in Medical Records Dumping Case, available at* http://www.hhs.gov/news/press/2014pres/06/20140623a.html (last updated June 23, 2014) (reaching a settlement with Parkview Health System after employees left 71 cardboard boxes of medical records on a retiring physicians driveway); *see* U.S. Dep't of Health and Human Servs., *Bulletin: HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software*, (Dec. 2014), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/acmhs/acmhsbulletin.pdf (reaching a $150,000 settlement with Anchorage Community Mental Health Services after the organization's computer systems became infected with malware, leading to the breach of ePHI for 2,743 individuals); *see* U.S. Dep't of Health and Human Servs., *Stolen Laptops Lead to Important HIPAA Settlements*, *available at* http://www.hhs.gov/news/press/2014pres/04/20140422b.html (last updated Apr. 22, 2014) (settling with QCA Health Plan for $250,000 and Concentra Health Services for $1.7 million after stolen laptops led to a breach. The breach led to investigations demonstrating both companies did not take substantial steps to protect their health information despite having knowledge of the faults in their security systems).

[6] U.S. Dep't of Health and Human Servcs., Office of Civil Rights, Resolution Agreement between OCR and Cornell Prescription Pharmacy 2015) *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cornell/cornell-press-release.html.

[7] *See* U.S. Dep't of Health and Human Srvcs., Office of Civil Rights, *Case Examples and Resolution Agreements*, *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/ (last visited June 18, 2015).

[8] Charles Ornstein, *Fines Remain Rare Even as Health Data Breaches Multiply*, ProPublica (Feb. 27, 2015) *available at* http://www.propublica.org/article/fines-remain-rare-even-as-health-data-breaches-multiply#.

[9] *See Your Health and Your Privacy: Protecting Health Information in a Digital World Before the Subcomm. On Privacy, Tech. and the Law of the S. Comm. on the Judiciary*, 112th Cong. (2011) (statement of Sen. Al Franken) (''[T]he overall record of [HIPAA] enforcement is simply not satisfactory''), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-112shrg87166/html/CHRG-112shrg87166.htm.

[10] *See U.S. Department of Health and Human Services, Office of the Inspector General Report: The Office for Civil Rights Did Not Meet All Federal Requirements in Its Oversight and Enforcement of the Health Insurance Portability and Accountability Act Security Rule* (Nov. 2013) (noting that ''OCR did not meet [certain] Federal requirements critical to the oversight and enforcement of the Security Rule'').

[11] 42 U.S.C. § 17939(c)(1) (2009).

[12] *See* 42 U.S.C. § 17940 (2010).

[13] *OCR Launches Phase 2 HIPAA Audit Program with Pre-Audit Screening Surveys*, McDermott Will & Emery (May 18, 2015), *available at* http://www.mwe.com/ocr-launches-phase-2-hipaa-audit-program-with-pre-audit-screening-surveys-05-18-2015/.

[14] Statement of Iliana Peters, OCR Senior Advisor for HIPAA Compliance and Enforcement, at Conference on Safeguarding Health Information: Building Assurance through HIPAA Security (Sept. 24, 2014).

   ISSN 1064-2137

FTC Data Privacy and Security Enforcement

Section 5 of the FTC Act as Jurisdictional Base. The FTC has entered the data privacy and security enforcement fray with gusto, relying primarily on Section 5 of the FTC Act[15] (the ''FTC Act'') as the jurisdictional base for its enforcement authority in this realm. Section 5 is a broadly written statute directed to ''unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce.'' The only parameters the statute on its face imposes on the FTC's enforcement authority are that, for the FTC to intervene: (a) the act or practice must be likely to cause a substantial injury to consumers that is not otherwise reasonably avoidable, and (2) the negative impact of the act must not be outweighed by countervailing benefits to consumers or competition.[16]

Neither the FTC Act nor any corresponding regulation or subsequent act of Congress either expressly grants the FTC jurisdiction over data practices or declares data practices as an unfair or deceptive act or practice affecting commerce in which the FTC may intervene. Whether the FTC Act nonetheless provides the FTC with such a jurisdictional base is the very bone of contention in *FTC v. Wyndham*.[17] In that case, the FTC sought an injunction against the hospitality entity Wyndham Worldwide for its alleged failure to provide sufficient security measures for personal data it collected and stored. The FTC claimed that this failure led to a large-scale hack from 2008 to 2010. Wyndham filed a motion to dismiss claiming, in relevant part, that: (a) the FTC lacked authority[18] to assert ''unfairness'' claims in the data security context because Congress has enacted other federal statutes to regulate and enforce data-security standards; and (b) applying Section 5 of the FTC Act to support data breach enforcement prior to the FTC's promulgation of corresponding regulations is a due process violation.[19] Pointing to the broad wording of Section 5 of the FTC Act, and articulating the view that the FTC needs flexibility in enforcing a dynamic field like data privacy), the district court denied Wyndham's motion, finding both that the other federal statutes regulating and enforcing data security standards can coexist with utilizing the FTC Act for data-security enforcement. The Third Circuit recently heard oral argument on Wyndham's appeal.[20]

In *LabMD v. FTC*, a similar case involving FTC data protection enforcement, this time in the health care industry, a medical laboratory providing cancer-screening services to physicians sought an injunction against the FTC's issuance of an administrative complaint alleging LabMD's improper public disclosure of protected health information through a peer-to-peer file sharing network.[21] In support of its claim, LabMD asserted defense theories identical to those in *Wyndham*; most notably that the FTC Act does not apply to disclosure of protected health information. The U.S. District Court for the Northern District of Georgia granted the FTC's motion to dismiss without any indication as to whether use of the FTC Act to enforce data security practices was a violation of LabMD's due process rights.[22] The administrative case is ongoing, as the FTC administrative law judge recently denied LabMD's motion to dismiss based on alleged due process violations and other arguments.[23]

The question of whether Section 5 of the FTC Act supports FTC jurisdiction over data breaches is an important one for the health care industry, which relies on the collection, storage and use of health data and other personal data. Final adjudications in *Wyndham*, *LabMD* and similar cases that likely will follow in their wake could have significant implications for health care organizations and the organizations that support them.

FTC's Health Data Breach Law for Non-Provider Health Industry Entities.[24] The FTC also has in its arsenal the data breach rules applicable to vendors of personal health records (PHR), PHR-related entities, and third-party service providers of vendors of PHRs and PHR-related entities. The FTC's rule requires entities to notify individuals promptly after gathering the necessary information concerning the breach and to notify the FTC within ten days of discovering the breach if the information involves more than 500 people; if the breach affects less than 500 people, the FTC requires notice within 60 calendar days following the end of the applicable calendar year. Finally, if the breach affects at least 500 residents of a given state, the entity must notify the media within 60 days after the breach and in any event without unreasonable delay. The breach notices provide a ready source of targets for investigations that could lead to further enforcement action by the FTC under Section 5 of the FTC Act.

Other Executive Branch Policy and Enforcement Activity

Recent Executive Orders. President Obama has issued two executive orders thus far in 2015 on the subject of data security practices. The first[25] promotes information sharing regarding cybersecurity amongst the private sector and the government and is designed to build upon the relationships between private industry and government agencies to facilitate better data security

[15] 15 U.S.C. § 45(a) (2012).
[16] 15 U.S.C. § 45(n) (2012).
[17] *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 613 (D.N.J. 2014).
[18] Wyndham based this argument on *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000), involving a statute that clearly contemplated a distinct regulatory scheme for tobacco products.
[19] *Wyndham*, 10 F. Supp. 3d at 622. Wyndham argued the pre-existing framework constituting the outer limits of the FTC's jurisdiction in data practices included the Fair Credit Reporting Act, 15 U.S.C. § 1681 (2003), the Gramm-Leach-Bliley Act, 15 U.S.C. § 94 (2012), and the Children's Online Privacy Protection Rule, 15 U.S.C. § 6501 *et seq*. (2003).
[20] *FTC v. Wyndham Worldwide Corp.*, 3d Cir., No. 14-3514.
[21] No. 1:14-cv-810, 2014 U.S. Dist. LEXIS 65090 (N.D. Ga. May 12, 2014).
[22] *Id.*
[23] 2015 FTC (LEXIS) 122 (May 26, 2015). LabMD separately filed a claim against Tiversa alleging Tiversa hacked into its computers and then mislead the FTC into believing a breach of patient data had occurred. *LabMD v. Tiversa Holding Corp.*, W.D. Pa, No. 2:15-cv-92. On June 19, 2015, LabMD requested the administrative court to refer the cybersecurity firm Tiversa Inc. to the Department of Justice.
[24] *Complying with the FTC's Health Breach Notification Rule*, Fed. Trade Comm'n., *available at* https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule.
[25] Exec. Order No. 13691, 80 Fed. Reg. 9347 (Feb. 13, 2015).

practices and prevent future breaches. The second deems cyberattacks a national emergency, and blocks the possessions of any individual engaged in cybercrime.[26]

U.S. Department of Justice. DOJ's Cyber Crimes unit has issued ''Best Practices for Victim Response and Reporting of Cyber Incidents.''[27] The best practices include guidance on: (a) proactively establishing plans and procedures to ensure the organization is well positioned to respond to a cyber incident; (b) executing on the organization's incident response plan when faced with a cyber incident; (c) actions that should be avoided following a cyber incident (e.g. refrain from using the compromised system and do not ''hack back'' or retaliate); and (d) post-incident review and remediation.

Federal Communications Commission. The FCC's recent involvement in consumer privacy is grounded in the Telephone Consumer Protection Act's (TCPA) prohibition against calls and messages to a mobile device using auto dialers and prerecorded messages from landlines without express written consent.[28] The TCPA prohibition received prominence in the health care context in *Mais v. Gulf Coast Collection Bureau, Inc.*,[29] a class action filed by a patient against a radiology provider and its billing agency and debt collection agent for debt collection calls to the patient's cell phone through a predictive dialer. Both the district court finding in the plaintiff's favor and the Eleventh Circuit's reversal focused on the validity of a 2008 FCC Declaratory Ruling that providing a cell phone number on a credit application constitutes consent for subsequent medical debt collection calls.[30] The district court had found the debt collector liable, holding that the declaratory ruling contradicted the clear meaning of the TCPA and that compliance with HIPAA is not tantamount to compliance with the TCPA. The Eleventh Circuit supported the validity of the ruling.[31] Particularly relevant to health care industry TCPA compliance planning is that the Eleventh Circuit characterized its decision that the TCPA permitted disclosure as consistent with HIPAA even though the plaintiff's cell phone number was included within the medical record information and thereby protected from disclosure under HIPAA.[32]

State Attorneys General Health Care Privacy and Data Security Enforcement. Relying on state consumer protection laws and their recent grant of HIPAA enforcement authority under the HITECH Act, attorneys general in several states have become active enforcers in privacy and data security. In May 2015, for example, Illinois Attorney General Lisa Madigan filed a lawsuit against FileFax, a Chicago document storage and destruction company, alleging that the company exposed thousands of medical records by improperly disposing of the records.[33] The suit alleges that a health care provider engaged FileFax to appropriately destroy medical records on its behalf, but the records were later ''discovered discarded in a dumpster outside of [FileFax's] office,'' and asserts a violation of the Illinois Personal Information Protection Act[34] and the Illinois Consumer Fraud and Deceptive Business Practices Act.[35]

In January, Indiana's attorney general settled a case involving alleged violations of the Indiana Disclosure of Security Breach Act and HIPAA by a local dentist.[36] This was the Indiana attorney general's first suit in response to a HIPAA violation. The dentist hired a records disposal company to retrieve and dispose of medical records. The attorney general alleged that, less than a week later, 63 boxes of patient medical records containing information on more than 5,600 patients were found in a dumpster. The dentist agreed to a consent judgment and payment of a $12,000 penalty.

Other recent and notable examples of state attorneys general enforcement in the health care context are reflected in various 2014 settlements: (1) the settlement by the Massachusetts attorney general with a hospital for $40,000 and certain corrective actions resulting from the theft of an unencrypted laptop containing protected health information of 2,159 patients;[37] (2) the settlement by the California attorney general with a leading health insurance provider for $150,000 plus policy and procedure changes resulting from allegations that the insurer took too long to notify more than 20,000 current and former employees of a 2011 data breach involving their personal information;[38] (3) the settlement by the Massachusetts attorney general with a health care system for $100,000 and certain corrective actions resulting from the theft of an unencrypted laptop containing protected health information and per-

[26] Exec. Order No. 133694, 80 Fed. Reg. 18077 (Apr. 1, 2015); *see also* Tom Syndor, *A Step in the Right Direction: New Executive Order Targets the Property of Foreign Cyberattackers*, TECH POLICY DAILY (Apr. 9, 2015), *available at* http://www.techpolicydaily.com/technology/a-step-in-the-right-direction-new-executive-order-targets-the-property-of-foreign-cyberattackers/ (explaining blocking property is effectively the impounding of property held in the United States, targeting foreign hackers).

[27] U.S. DEP'T OF JUS., CYBERSECURITY UNIT, BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS (2015), *available at* http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf.

[28] 47 U.S.C. § 227 *et seq.*; 27 FCC Rcd. 1830 (2012); 45 C.F.R. § 160.103 (2013); 47 C.F.R. § 64.1200(a)(2) (2012); 47 C.F.R. § 64.1200(a)(3)(v) (2012).

[29] 768 F.3d 1110 (11th Cir. 2014).

[30] 27 FCC Rcd. 1830 (2012).

[31] 768 F.3d at 1119. The Eleventh Circuit ruled that that the district court lacked jurisdiction to address the validity of the 2008 FCC Ruling because any case challenging the validity of FCC orders must be brought directly to federal appellate courts under the Hobbs Act.

[32] *Id.* at 1125-1126.

[33] *See Madigan Sues Chicago Area Company for Medical Record Data Breach*, ILL. ATT'Y GEN. (May 6, 2015), *available at* http://www.illinoisattorneygeneral.gov/pressroom/2015_05/20150506.html.

[34] 815 Ill. Comp. Stat. § 530 *et seq* (2006).

[35] 815 Ill Comp. Stat. § 505 *et seq* (2010).

[36] *See State Settles with Former Dentist Accused of Dumping Patient Files*OFFICE OF THE IND. ATT'Y GEN. (Jan. 9, 2015), *available at* http://www.in.gov/activecalendar/EventList.aspx?fromdate=1/1/2015&todate=1/31/2015&display=Month&type=public&eventidn=203146&view=EventDetails&information_id=210192.

[37] *See Boston Children's Hospital Settles Data Breach Allegations*, MASS. ATT'Y GEN. (Dec. 19, 2014), *available at* http://www.mass.gov/ago/news-and-updates/press-releases/2014/2014-12-19-boston-childrens.html.

[38] *See Attorney General Kamala D. Harris Announces Settlement with Anthem Blue Cross over Data Breach*, CAL. DEP'T OF JUS. (Oct. 1, 2012), *available at* https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-settlement-anthem-blue-cross-over.

   ISSN 1064-2137

sonal information of approximately 4,000 individuals;[39] and (4) the settlement by the Massachusetts attorney general with a Rhode Island hospital for $150,000 resulting from the loss of unencrypted back-up tapes allegedly containing personal and protected health information of approximately 12,000 Massachusetts residents.[40]

Private Actions Triggered by Data Breaches

Data breaches have also triggered private lawsuits, increasingly ones brought as class actions, in both federal and state court. Following is a discussion of the salient litigation and compliance risk management insights emerging from some of the leading cases.

Legal Theories Supporting the Claims. The menu of legal theories asserted by plaintiffs in these cases seems limitless, as they include among others: (c) violation of various federal statutes (e.g, Fair Credit Reporting Act (FCRA),[41] the Privacy Act of 1974,[42] Graham Leach Blilely Act (GLBA),[43] and Children' Online Privacy Protection Act (COPPA),[44] Federal Declaratory Judgment Act;[45] (b) violations of state statutes (e.g., data breach statutes, health and personal data protection statutes, patient rights statutes, medical professional and hospital licensure statutes) consumer protection statutes (fraud and deceptive practices and unfair trade or competition); and (c) state common law claims (e.g., negligence/gross negligence/negligence *per se*, invasion of privacy, identity theft, misappropriation of confidential financial information, breach of fiduciary duty, consumer fraud, negligent misrepresentation (e.g., by omission), breach of contract and implied contract, breach of covenant of good faith and fair dealing, detrimental reliance, and infliction of emotional distress).[46]

The Standing Hurdle. Regardless of the statute or common law theory underlying a data breach claim, plaintiffs are likely to face a motion to dismiss for lack of standing in both federal and state court. The standing challenges have been front and center in various prominent data breach cases decided by both federal and state courts since the U.S. Supreme Court's 2013 ruling in *Clapper v. Amnesty International USA*.[47] These cases provide valuable insights for crafting any data breach litigation strategy (on either side of the case) and for any privacy and security compliance program planning and risk management endeavor.

1. Article III Underpinnings. Article III of the U.S. Constitution empowers the federal courts to hear only ''cases and ''controversies.'' For at least two decades, the U.S. Supreme Court has interpreted this provision to require that plaintiffs seeking relief in federal court must allege injury that is: (a) a concrete and particularized injury in fact, (b) traceable to the defendant's acts or omissions, and (c) able to be redressed by a judicial decision.[48] The Court's 2013 ruling in *Clapper* introduced what is arguably a higher burden of proof for satisfying the ''injury in fact'' prong of the analysis.

2. *Clapper.* In *Clapper*, the plaintiffs sought relief under a post-911 federal statute authorizing foreign intelligence surveillance.[49] In support of its reversal of the U.S. Court of Appeals for the Second Circuit's denial of the defendant's motion to dismiss for lack of standing under the cases and controversies provision of Article III, the Supreme Court ruled that, a ''threatened injury must be *certainly impending* to constitute injury in fact'' and that ''allegations of *possible* future injury'' are insufficient.[50] Applying these principles to the facts of that case, the Court found not only that the injury had not yet occurred, but that the claim was based on a mere fear of injury that was ''highly speculative'' and dependent upon a ''highly attenuated chain of possibilities.''[51] The Court admonished that plaintiffs ''cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.''[52] The alleged harm the *Clapper* Court characterized as ''self-inflicted'' was the plaintiffs' incurrence of costs in response to their fear of government surveillance, including travel costs for in-person meetings in foreign coun-

---

[39] *See Beth Israel Deaconess Medical Center to Pay $100,000 Over Data Breach Allegations*, MASS. ATT'Y GEN. (Nov. 21, 2014), *available at* http://www.mass.gov/ago/news-and-updates/press-releases/2014/2014-11-21-beth-israel-data-breach.html.

[40] *SeeWomen & Infants Hospital to Pay $150,000 to Settle Data Breach Allegations Involving Massachusetts Patients*, MASS. ATT'Y GEN. (July 23, 2014), *available at* http://www.mass.gov/ago/news-and-updates/press-releases/2014/2014-07-23-women-infants-hospital.html).

[41] 15 U.S.C. § 1681 (2003).

[42] 5 U.S.C. § 552a.

[43] 15 U.S.C. § 94 (2012).

[44] 15 U.S.C. § 6501 *et seq* (2003).

[45] 28 U.S.C. § 2201 (2006).

[46] *See, e.g., In re Sony Gaming Networks and Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942 (S.D. Cal. 2014), in which eleven plaintiffs from nine different states alleged 51 independent causes of action. Sony settled the case for $15 million in non-cash compensation (e.g., free games, game currency and subscription benefits), another $4 million for attorney fees, and notice of the settlement to potential class members. *See Peters v. St. Joseph Servcs. Corp.*, No. 4:14-cv-2872, 2015 U.S. Dist. LEXIS 16451; *In re Target Corp. Customer Security Data Breach Litig.*, 2014 U.S. Dist. LEXIS 175768 (D. Minn. Dec. 18, 2014) (finding that the plaintiffs had alleged sufficient harm in support of certain claims to deny the motion to dismiss). Target thereafter successfully settled the consumer case for $10 million, with final objections to the settlement being due on Nov. 10, 2015. *See* Hiroko Tabuchi, *$10 Million Settlement in Target Data Breach gets Preliminary Approval*, N.Y. TIMES, Mar. 19, 2015, *available at* http://www.nytimes.com/2015/03/20/business/target-settlement-on-data-breach.html?_r=0. As of May, 2015, Target's settlement agreement with Mastercard for $19 million for a separate suit brought by financial institutions had fallen through. *See* Elizabeth Weise, *Target Breach Settlement with MasterCard Falls Through*, USA TODAY, (May 22, 2015), *available at* http://www.usatoday.com/story/tech/2015/05/22/target-breach-mastercard-visa/27782665.

[47] 133 S.Ct. 1138 (U.S. 2013). The case dealt with the Foreign Intelligence Surveillance Act Amendments of 2008 that created a new framework under which the federal government could seek the Foreign Intelligence Surveillance Court's authorization of surveillance targeting communications of non-U.S. citizens abroad.

[48] *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992); *see also Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139 (2010); *see Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007) (establishing the requirement that pleadings must first pass the line of possibility to plausibility).

[49] The Foreign Intelligence Surveillance Act Amendments of 2008, 50 U.S.C. § 1881(a) (2008).

[50] *Clapper*, 133 S. Ct. 1138 at 1147.

[51] *Id.*

[52] *Id.* at 1151.

tries in lieu of virtual communications through electronic means.[53]

3. *Clapper's* Data Breach Progeny. The standing issue has surfaced in several prominent, post-*Clapper* data breach cases in which both federal and state courts have applied the *Clapper* threat of harm standard for determining standing, or some variation of it.[54] These and several other cases are still pending in federal district courts[55] merit close consideration in any data breach risk management endeavor and in any industry context, including the health care industry.

Following the lead of the *Clapper* and its antecedents, state courts have applied a similar standing analysis to data breach claims, focusing generally on whether the plaintiff's allegations were sufficient to demonstrate both an ''injury in fact'' and a ''causal connection'' between the alleged injury and the defendant's acts or omissions.[56] What seems universal among the courts is that the mere threat of harm is not enough. In some of these cases, the courts applied the same ''concrete and particularized,'' ''certain,'' ''imminent'' or ''certainly impending[57] standards enunciated in *Clapper* and its antecedents for determining whether an alleged risk of harm presented a sufficient risk, and were not deterred by the fact that the *Clapper* standard arose in the context of claims involving constitutional challenges to a federal statute enacted for national security reasons.[58] In other cases, the courts have applied variations of the *Clapper* risk of harm standard; for some courts, a threat of harm that was ''certainly impending'' was sufficient, while others were satisfied by a threat that was either ''credible of being impending'' or ''plausibly impending.''[59] These variations are subtle at best, will likely be difficult to apply, and could lead to inconsistent outcomes on the standing issue under the same or similar sets of facts.

Particularly notable for health care industry stakeholders is *Tabata v. Charleston Area Med. Ctr., Inc.*,[60] in which the West Virginia Supreme Court of Appeals ruled that patients whose information was inadvertently published by a medical center on the internet for more than six months (but never shown to have been accessed by others) had standing because they had a ''legal interest in having their medical information kept confidential'' that is ''concrete, particularized, and actual,'' and ''[w]hen a medical professional violates this right, it is an invasion of the patient's legally protected

[53] Notably, in his dissenting opinion, Justice Stephen G. Breyer found the totality of circumstances indicated an imminent harm to the plaintiffs, highlighting various factors as indicative of the harm being imminent and not speculative: the government's likelihood of intercepting some of plaintiffs' communications under Section 1881(a), past government behavior, the government's capacity and strong motivation to conduct electronic surveillance. *Id.* at 1159 (Breyer, J. dissenting).

[54] *See, e.g., In re Sci. Applications Int'l Corp. Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14 (D.D.C. 2014) (a class action arising from the theft of tapes from the car of an SAIC employee that contained personal and medical records of 4.7 million U.S. military members enrolled in a federal health benefit program); *In re Adobe Systems Inc. Privacy Litig.*, No. 13-cv-5226, 2014 U.S. Dist. LEXIS 124126 (N.D. Cal. Sept. 4, 2014) (breach of customer data collected by Adobe and Adobe source code stored on the company's servers for several weeks without detection. Adobe appealed the denial of its motion to dismiss to the 9th Circuit, but the parties settled prior to oral argument); *Sony*, 996 F. Supp. 2d 942 (S.D. Cal. 2014) (hackers gained access to Sony's Playstation Network and stole the personal data (e.g., names, mailing addresses, birth dates, and credit card numbers) on the network that Sony had collected from millions of Sony customers when they signed up to participate in the network); *Target,* 2014 U.S. Dist. LEXIS 175768 (D. Minn. Dec. 18, 2014) (access by hackers to credit and debit card information of close to 110 million Target customers during the 2013 holiday shopping season); *Peters,* No. 4:14-cv-2872, 2015 U.S. Dist. LEXIS 16451 (S.D. Tex. Feb. 11, 2015) (a class of plaintiffs filed a lawsuit against St. Joseph's Health System after its computer network was hacked; *see In re Barnes & Noble PIN Pad Litigation,* No. 12-cv-8617, 2013 U.S. Dist. LEXIS 125730 (N.D. Ill. Sept. 3, 2013). Several cases have appeals pending before the Seventh Circuit.

[55] *See, e.g., Remijas v. Neiman Marcus Group, LLC,* No. 14-cv-1735, 2014 U.S. Dist. LEXIS 129574 (N.D. Ill. Sept. 16, 2014) (dismissed); *see Lewert v. P.F. Chang's China Bistro, Inc.*, No. 14-cv-4787, 2014 U.S. Dist. LEXIS 171142 (N.D. Ill. Dec. 10, 2014) (dismissed); *see Tierney v. Advocate Health & Hosp. Corp.*, No. 13-cv-6237, 2014 U.S. Dist. LEXIS 158750 (N.D. Ill. Sep. 4, 2014) (arising within the health care context, utilizing *Clapper*, and finding the hospital could not be sued under the FCRA).

[56] For example, the standard analysis historically applied by Illinois state courts requires a ''distinct and palpable'' injury fairly traceable to the defendant's conduct and redressable by court action. *Greer v. Ill. House. Dev. Auth.,* 122 Ill. 2d. 463, 492-93 (1988). In *Maglio v. Advocate Health & Hosps. Corp.*, No. 13-CH-2701, 2015 Ill. App. Unpub. LEXIS 1190 at *15 (Ill. App. Ct. July 10, 2014), the court expressly noted that ''Federal standing principles are similar to those in Illinois, and the case law is instructive.''

[57] 15 U.S.C. § 45(n) (2012).

[58] The *Sony* court found that there was an absence of any indication in *Clapper* that the Supreme Court intended a wide-reaching revision to existing standing doctrine. The *Sony* court was reluctant to conclude that *Clapper* represented the sea of change that Sony suggested in its motion to dismiss and found that the ''credible threat of impending harm'' arising from the disclosure of PHI following the breach was sufficient even in the absence of proof of actual third-party access to the PHI. *Sony*, 996 F. Supp. 2d 942, 961 (S.D. Cal. 2014). Similarly, the *Adobe* court noted the extent of the Supreme Court's standing analysis when determining the constitutionality of actions taken by the Federal Government. *Adobe*, 2014 U.S. Dist. LEXIS 124126 at *24 (quoting *Clapper*, 133 S.Ct. at 1147) (''[o]ur standing inquiry has been especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional.'' (alteration omitted) (internal quotation marks omitted)). According to the *Adobe* court, *Clapper* ''did not change the law governing Article III standing.'' *Adobe*, 2014 U.S. Dist. LEXIS 124126 at *24. The Supreme Court neither overruled any precedent nor ''reformulate[ed] the familiar standing requirements of injury-in-fact, causation, and redressability, but instead, *Clapper* merely held that the Second Circuit had strayed from these well-established standing principles by accepting a too-speculative theory of future injury.'' (internal citations omitted) *Id.* (citing *Clapper,* 133 S. Ct. at 1146 as ''characterizing the Second Circuit's view of standing as 'novel' '') The *Adobe* court was similarly reluctant to conclude that *Clapper* represents a sea change and further noted that *Clapper* ''arose in the sensitive context of a claim that other branches of government were violating the Constitution, and the U.S. Supreme Court itself noted that its standing analysis was unusually rigorous as a result.'' *Id.* (citing *Clapper*, 133. S. Ct. at 1147); *see also Moyer v. Michaels Stores, Inc.*, No. 14 C 561, 2014 U.S. Dist. LEXIS 965888 (N.D. Ill. July 14, 2014) (voicing the same view).

[59] *See Adobe*, 2014 U.S. Dist. LEXIS 124126 at *43.

[60] 759 S.E.2d 459 (W. Va. 2014).

   ISSN 1064-2137

interest.'' On its face, this ruling might be read as the equivalent of a ''per se'' standing theory based on a mere violation of legal interest right arising from a statutory or common law right, regardless of whether the violation resulted in harm. However, the degree of risk that the long-term and highly public nature of the disclosure would lead to actual access to the information resulting from the breach is likely to have been a key factor in the court's eyes. At least one state court has already found the *Tabata* court's standing analysis to be less persuasive than that of the leading federal cases,[61] but it may be too soon to tell whether the case will consistently be viewed as an outlier.

4. Adequacy of the Harm to Support a Claim. The types of threatened harm identified in data breach cases filed since *Clapper* included, among others: (a) identity theft or increased risk of identity theft, (b) costs incurred to mitigate the risk of identity theft, (c) loss of privacy through the exposure of personal information; (d) loss of the value of personal and medical information, (e) loss of the value of payments made to the defendant that should have been used to pay for proper security measures, (f) the loss of right to truthful information about the security of their data, data security, (g) expenses incurred to remediate breaches (e.g., a bank's costs to issue new credit cards, respond to customer complaints, and absorb the amount of fraudulent credits transactions, and on the credit card holder's side, bank charges for fraudulent transactions and lost access to accounts).[62]

Among the most notable facts and circumstances the courts have considered in determining whether the alleged harm was sufficient to meet the ''injury in fact'' requirement are: (a) whether the breach arose from third party hacking, physical burglary (e.g., laptops stolen from cars, discs stolen in the course of a physical break-in) and the characteristics of the perpetrators of a breach:[63] (b) whether the breach arose from an inadvertent public disclosure by the defendant; (c) how difficult it would be for third parties to actually access the information contained on stolen laptops, tapes or other stolen media;[64] (d) whether the personal data was ultimately accessed, disclosed or used by a third party;[65] (e) whether the personal data was public disseminated (e.g., on the internet) and for how long; (f) what standards the defendants' security and other safeguards met (e.g., HIPAA, industry standards, best practices);[66] (g) whether the defendant had a contractual obligation (express or implied) to safeguard the plaintiff's personal information;[67] (h) how quickly the defendant discovered the breach, remediated the breach and notified the affected individuals of the breach;[68] and (i) whether the personal data was medical or health care related data.

HIPAA's Influence on the ''Standard of Care'' Applied in Data Breach Cases. While HIPAA provides no private rights of action, a handful of state courts have found that HIPAA may be utilized to inform the standard of care for state law negligence claims.[69] *Byrne v. Avery Center for Obstetrics and Gynecology*, decided recently by the Connecticut Supreme Court, is illustrative.[70] *Byrne* involved a patient who sued her health care provider alleging breach of contract and negligent disclosure claims resulting from the provider's disclosure of the patient's medical records in response to a subpoena by the patient's ex-boyfriend in the context of a paternity lawsuit that resulted in his ability to review the medical record. The health care provider's HIPAA Notice of Privacy Practices stated that it would not disclose patients' protected health information without the patient's authorization; in addition, the plaintiff had also expressly requested that the health care provider not disclose her medical information to her ex-boyfriend. The patient based her negligent disclosure claim on the health care provider's alleged failure to follow the duty of care prescribed by HIPAA for protected health information. The court concluded that using HIPAA to inform the standard of care in a negligence suit against the provider did not interfere with the objectives of HIPAA.[71]

Cases Based on Violation of Federal Statutes Not Dependent on Proof of Harm. A number of data breach lawsuits have included claims for violation of federal statutes, some of which allow for statutory damages absent proof of actual harm.[72] *Clapper's* primary focus on proof of actual or imminent injury to determine standing in federal court may have little influence in a court's determination of standing in cases involving such federal laws.

Most notable among recent cases is *Spokeo Inc. v. Robins*,[73] which focuses primarily on whether proof of

[61] 2015 Ill. App. 2d. App140782-U, 2015 Ill. App. Unpub. LEXIS 1190.

[62] *See, e.g.*, *In re Sci. Applications*, 45 F. Supp. 3d 14 (2014).

[63] *See, e.g.*, *Adobe*, 13-cv-05226-LHK, 2014 U.S. Dist. LEXIS 124126 (N.D. Cal. Sept. 4, 2014), in which the court also considered the fact that the perpetrators used Adobe's own systems to perpetrate the theft.

[64] *See, e.g.*, In re Sci. Applications, 45 F. Supp.3d 14 at 28 (in which the court noted that it would be extremely difficult to read the data on the tapes given the software and hardware required to gain access to the information stored).

[65] *See*, *e.g.*, In re Sci. Applications, 45 F. Supp.3d 14 at 28-29.

[66] *See, e.g.*, Adobe, 2014 U.S. Dist. LEXIS 124126 (N.D. Cal. Sept. 4, 2014).

[67] *Id.*

[68] *See, e.g.*, Peters, 2015 U.S. Dist. LEXIS 16451 (St. Joseph's shut down the affected technology and conducted an internal investigation that uncovered no evidence that any data, including protected health information, had been misused).

[69] *See e.g.*, *RK v. St. Mary's Med. Ctr. Inc.*, 735 S.E.2d 715 (W. Va. 2012); *I.S. v. Wash. Univ.*, No. 4:11-cv-235SNLJ, 2011 U.S. Dist. LEXIS 66043 (E.D. Mo. June 14, 2011); *Harmon v. Maury Cnty. Tenn.*, No. 1:05-cv-26, 2005 U.S. Dist. LEXIS 48094 (M.D. Tenn. Aug 31, 2005); *Yath v. Fairway Clinics NP*, 767 N.W.2d. 34 (Minn. Ct. App. 2009); and *Acosta v. Byrum*, 638 S.E.2d. 246 (N.C. Ct. App. 2006).

[70] *Byrne v. Avery Ctr. for Obstetrics and Gynecology, P.C.*, 102 A.3d 32 (Conn. 2014).

[71] We note also, *Hinchy v. Walgreen Co.*, 21 N.E.3d 99 (Ind. Ct. App. 2014) in which the Indiana Court of Appeals held an employer responsible, under the common law theories of negligence and *respondeat superior*, for the HIPAA violation of one of its employees for improper access to protected health information.

[72] *See, e.g.*, *Tierney v. Advocate Health & Hosp. Corp.*, No. 13-cv-6237, 2014 U.S. Dist. LEXIS 158750 (N.D. Ill. Sep. 4, 2014) (health care context, utilizing *Clapper*, finding the hospital could not be sued under the FCRA); *Maglio v. Advocate Health & Hosps. Corp.*, No. 13-CH-2701 (Ill 16th Cir. July 10, 2014); *Vides v. Advocate Health & Hosps. Corp.*, No. 13-CH-2701 (Ill 16th Cir. May 27, 2014).

[73] 742 F.3d 409 (9th Cir. 2014), *cert. granted*, 83 U.S.L.W. 3819 (U.S. Apr. 25, 2015) (No. 13-1339).

actual or imminent harm is necessary to demonstrate standing for a violation of the FCRA. The claim arose from publication of the plaintiff's personal information through the Spokeo.com search engine that gathers personal data from publicly available sources (e.g., their contact information, age, health, and occupation). The plaintiff alleged that he suffered emotional and financial harm from the publication when his ability to obtain employment was hurt after Spokeo published inaccurate information about him. The district court had held that allegations of possible future injury do not satisfy the standing requirements.[74] The Ninth Circuit Court of Appeals reversed, ruling that proof of damages is unnecessary to sustain a cause of action under the Fair Credit Reporting Act because a plaintiff may suffer an ''injury in fact'' under the statutory right without suffering actual damages.[75] Under the Ninth Circuit's holding, therefore, a plaintiff must demonstrate that Spokeo violated his statutory right, but does not need to demonstrate that he suffered damages. The U.S. Supreme Court granted review in April 2015 and will hear and decide upon *Spokeo* in its next term. The ultimate Supreme Court decision could have significant implications for standing privacy cases based on claims of violations of federal statutes that assume injury in fact resulting from a violation of a statutory right itself and do not require proof of either actual or threatened harm.[76]

Observations, Conclusions and Recommendations

Now more than ever, health care organizations are faced with managing the significant risk of constant data security incidents that are or may lead to actionable breaches. Indeed, responding to data security occurrences and the multi-faceted fall-out of data-breaches may now be the ''new normal.'' Recent developments and trends in the data breach realm provide valuable risk prevention and risk management insights.

Clearly, health care organizations will have to deal with more than HIPAA oversight and enforcement by OCR. What typically follows in the wake of data breach incidents is a ''perfect storm'' on the enterprise risk management front—immediate steps to correct the problem and prevent further breaches; assessing whether notices to the affected individuals and the government are needed and preparing and sending those notices; responding to relentless media scrutiny; defending intense and aggressive government audits, investigations and enforcement actions by OCR, FTC and others; and litigating private class actions—all of which sap the organization of valuable and sometimes scarce human and financial resources. Preventing government and private actions from being filed is virtually impossible and, while they may never be fully adjudicated either in an administrative or judicial forum, such actions can result in fines and monetary settlements and surely lead to the incurrence of significant legal expenses.[77] And, of course, the potential reputational damage from prominent media coverage could be the most devastating of all consequences.

As in any dimension of enterprise risk, it is impossible to entirely eliminate the risk. The key to effective data breach risk management is to develop and apply a formula that focuses on proactive measures that prevent the occurrence of a data breach and establish a robust mitigation strategy to stem the adverse effects of any breach that does occur. Fortunately, the formula will be the same tried and true formula that health care organizations have used to manage many other dimensions of legal and regulatory compliance risk: establish and maintain a data security and privacy compliance program that is effective in preventing and promptly detecting and remediating breaches, in monitoring compliance with the program, enforcing the program and continually improving the program.

In addition to reducing the likelihood that a breach will occur, an effective compliance program should position an organization, in the event of a breach to: (a) demonstrate that it has a robust and effective data protection program designed reasonably to protect the privacy and security of patients' health and other personal data; and (b) act quickly to stop the breach, prevent further breaches, identify the source of the breach and the data affected, prevent public dissemination of the data, prevent actual access to or misuse of the data and provide voluntary or required notices to the affected individuals and government agencies.

Rigorous and scrupulous compliance with HIPAA's privacy and security standards will go a long way toward the implementation of a robust privacy and data security compliance program for health care organizations. A key ingredient in a HIPAA compliance formula is conducting periodic, comprehensive HIPAA Security Rule risk analyses, documenting them, developing a remediation plan to address the findings, and executing on that plan.[78] OCR has repeatedly identified the lack of a comprehensive risk analysis of the potential vulnerabilities to the security safeguards for an organization's electronic protected health information as a widespread compliance weakness. According to OCR Director Samuels, OCR ''continue[s] to see a lack of comprehensive and enterprise-wide risk analysis and risk management that leads to major breaches and other compli-

[74] The district court cited *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992), rather than *Clapper*, in support of its analysis.

[75] 742 F.3d at 413.

[76] Wystan Ackerman, *Spokeo, Inc. v. Robins: Supreme Court to Decide Class Action Standing Issue,* JD Supra (May 4, 2015), *available at* http://www.jdsupra.com/legalnews/spokeo-inc-v-robins-supreme-court-to-41321/.

[77] *See, generally*, Ponemon Inst., 2015 Cost of Data Breach Study: Global Analysis (2015).

[78] *See Office of the Nat'l Coordinator for Health Info. Tech., Guide to Privacy and Security of Electronic Health Information* (2015), *available at* http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf (emphasizing the importance of following this assessment process); U.S. Dep't of Health and Human Servcs., Office of Civil Rights, Guidance on Risk Analysis requirements Under the HIPAA Security Rule (2010), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf. ONC also created as a downloadable application a security assessment tool geared toward assisting small businesses in their security compliance efforts. *See* Office of the Nat'l Coordinator for Health Info. Tech., *Security Risk Assessment*, *available at* http://www.healthit.gov/providers-professionals/security-risk-assessment (providing a downloadable risk assessment tool) (last visited June 23, 2015).

   ISSN 1064-2137

ance problems.''[79] In fact, OCR found that nearly 70% of the covered entities audited in the first phase of OCR audits did not have a complete and accurate security risk analysis,[80] and, in every case involving a breach of electronic protected health information that resulted in financial settlements with OCR since 2014, OCR required the covered entity to conduct a risk analysis as a component of the corrective action plan.[81]

Other prudent data breach compliance and liability prevention and risk management measures reflected in HIPAA and agency guidance for HIPAA compliance include following:

- Review the extent to which the organization has implemented HIPAA's ''addressable'' Security Rule implementation standards for any information systems or facilities with access to electronic protected health information, and, for any that were not implemented, document: (i) why any such addressable implementation standard was not reasonable and appropriate and (ii) all alternative security measures that were implemented;

- Confirm that the organization maintains an inventory of information system assets, including mobile devices;

- Confirm that all systems and software that transmit protected health information or personal information employ required encryption technology (covered entities and business associates who choose not to employ encryption must document the risk analysis supporting the decision not to employ encryption);

- Proactively identify and document potential threats (including all threat and vulnerability combinations), assess and document the likelihood/risk of a threat occurring, determine and document the likely impact on systems and the likely costs, and determine and document corrective actions that will improve prevention and mitigate risks;

- Prepare for a potential data breach (e.g., conduct a table top exercise to evaluate how the organization would perform in the event of an actual breach; consider lining up forensic firms, credit monitoring vendors and other breach vendors before an incident occurs);

- Confirm that the organization has adopted a disaster recovery and business continuity plan for each physical location that stores or otherwise has access to protected health information or personal information;

- Test the adequacy of other aspects of HIPAA security compliance using the audit protocol OCR used in its first phase of HIPAA audits[82] and the one developed by OCR for use in its second phase of HIPAA audits when it becomes available.

- Establish and maintain a comprehensive set of privacy, security and breach notification policies and procedures;

- Appropriately train workforce members on the organization's policies and procedures and document that training;

- Review and, if necessary, update the organization's website privacy policy and terms of use, notice of privacy practices and consent forms to meet regulatory requirements and accurately reflects the organizations current practices; and

- Execute HIPAA-compliant business associate agreements and update them on a periodic basis.

---

[79] Jocelyn Samuels, Director, Office for Civil Rights, address at Safeguarding Health Information: Building Assurance through HIPAA Security conference (Sept. 23, 2014).

[80] *OCR Lessons Learned from OCR Privacy and Security Audits*, U.S. DEP'T OF HEALTH AND HUMAN SRVCS. (March 7, 2013), *available at* https://privacyassociation.org/media/presentations/13Summit/S13_Lessons_Learned_OCR_PPT.pdf.

[81] *See* U.S. Dep't of Health and Human Servs., *County Government Settles Potential HIPAA Violations*, *available at* http://www.hhs.gov/news/press/2014pres/03/20140307a.html (last updated Mar. 7, 2014); *see* U.S. Dep't of Health and Human Servs., *Stolen Laptops Lead to Important HIPAA Settlements*, *available at* http://www.hhs.gov/news/press/2014pres/04/20140422b.html (last updated Apr. 22, 2014); *see* U.S. Dep't of Health and Human Servs., *County Government Settles Potential HIPAA Violations*, *available at* http://www.hhs.gov/news/press/2014pres/03/20140307a.html (last updated Mar. 7, 2014); *see* U.S. Dep't of Health and Human Servs., *Bulletin: HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software*, Dec. 2014, *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/acmhs/acmhsbulletin.pdf.

[82] U.S. Dep't of Health & Human Srvcs., *Health Information Privacy: Audit Program*, *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html (last visited June 23, 2015).