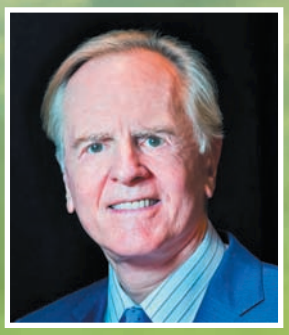
PUBLISHED BY 7X24 EXCHANGE INTERNATIONAL

7X24 Exchange INTERNATIONAL

1989 – 2014

25TH ANNIVERSARY

THE END-TO-END RELIABILITY FORUM™



John Sculley

2014 SPRING CONFERENCE

KEYNOTE SPEAKER

DIGITAL REALTY'S

Emphasizing Operational Consistency Across a Global Portfolio

ASHBURN CAMPUS

by Tatiana Melnik

HIPAA, NOT JUST FOR DOCTORS: TECHNOLOGY VENDOR RISKS & OBLIGATIONS

Over the last several years, and certainly since the numerous disclosures made by Edward J. Snowden regarding snooping by the U.S. Government, privacy and security issues have taken on a renewed importance. Nowhere is that more true than in the healthcare space, where, in 2009, Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act mandating penalties for healthcare related privacy and security breaches and expanding the scope of direct enforcement beyond healthcare providers to encompass information technology vendors serving the healthcare industry. Since the enactment of the HITECH Act, the Office of Civil Rights has taken action against fourteen different organizations and government entities reaching settlements and issuing fines totaling approximately $14.9 million. There has also been an increase in enforcement actions by the Federal Trade Commission and State Attorneys' General as well as plaintiffs by way of class action litigation.

A Bit of History

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[1] was one of the first laws to address the privacy of healthcare information. The goal of the law was to improve the efficiency and effectiveness of the healthcare system by, among other things, standardizing the electronic exchange of administrative and financial data[2]. In enacting HIPAA, Congress recognized that, "[h]ealth information is considered relatively 'safe' today, not because it is secure, but because it is difficult to access"[3] and enabling electronic transactions would, invariably, jeopardize the privacy and security of healthcare information. Congress therefore directed the Secretary of Health and Human Services (HHS) to adopt certain standards to protect the integrity, confidentiality, and security of health information.

Thirteen years after it enacted HIPAA, Congress revisited the privacy and security of healthcare information and enacted the HITECH Act as part of the American Recovery and Reinvestment Act of 2009.[4] This new law was, in part, a response to the lack of HIPAA enforcement[5] as well as a recognition that privacy and security concerns would increase with the move to electronic healthcare records.[6] In an effort to encourage increased HIPAA compliance and enforcement, the HITECH Act requires mandatory breach notification, sets forth a tiered civil penalty structure, and grants state Attorneys' General the right to enforce HIPAA on behalf of their state citizens. The HITECH Act also made clear that vendors that obtain or create protected health information on behalf of their healthcare clients are also subject to compliance with certain requirements of the HIPAA Laws. The HITECH Act therefore increased the financial risks for *all* organizations handling protected health information who fail to comply with HIPAA.

Currently, the scope of "HIPAA" includes the HIPAA statute passed in 1996, the HITECH Act, the Genetic Information Nondiscrimination Act (GINA) and four implementing federal regulations issued by HHS—the Privacy Rule, the Security Rule, the Breach Notification Rule, and the Enforcement Rule, commonly known as the "HIPAA Rules." To account for the changes required under the HITECH Act and GINA, HHS revised the HIPAA Rules and reissued them in the form of an "Omnibus Rule" on January 25, 2013 with an effective date of March 26, 2013.[7] Compliance was required by September 23, 2013.

Who is Subject to HIPAA and Where do Information Technology Vendors Fit?

Broadly speaking, HIPAA applies to entities and individuals handling or otherwise having access to "protected health information" (PHI). More specifically, "covered entities," "business associates" and their "subcontractors" are subject to HIPAA compliance. The three terms are defined in the HIPAA Rules.[8] Put simply,

- 'covered entities' are healthcare providers, health plans, and healthcare clearinghouses (referred to in this article simply as healthcare providers);
- 'business associates' are entities that provide services to covered entities *and* create, receive, maintain, or transmit PHI; and
- 'subcontractors' are those entities that provide services to business associates *and* create, receive, maintain, or transmit PHI.

PHI is defined broadly to encompass any information that allows someone to (i) link an individual with his or her physical or mental health condition, (ii) the provision of healthcare services, or (iii) the payment for healthcare services.[9]

Depending on where information technology (IT) vendors fall in the scheme of a particular transaction, they will be either business associates or subcontractors. In the Omnibus Rule, HHS made clear that 'business associate' includes entities that maintain PHI, "even if the [entities do] not actually view the PHI."[10] But, not all IT vendors are subject to HIPAA compliance. Some qualify for the so-called 'conduit exception,' when the vendor "transports information but does not access it other than on a random or infrequent basis as necessary to perform the transportation service or as required by other law."[11] The conduit exception is *narrow* and "is intended to exclude *only* those entities providing mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers (ISPs) providing mere data transmission services."[12] In distinguishing conduits from other IT vendors, HHS specifically advised that, "a data storage company that has access to [PHI] (whether digital or hard copy) qualifies as a business associate, ***even if the entity does not view the information or only does so on a random or infrequent basis.***"[13] As such, data centers and most other IT vendors that touch on PHI in performing services for healthcare providers or their business associates are subject to HIPAA compliance.

Direct Enforcement and Financial Responsibility

The Office of Civil Rights (OCR) is a component of the Department of Health and Human Services. OCR serves as the federal enforcer of HIPAA for all civil remedies. While rarely used, HIPAA does include criminal provisions, which are enforced by the Department of Justice. Further, the HITECH Act granted permission to the State Attorneys' General to enforce HIPAA on behalf of their citizens as *parens patriae*.

Prior to the HITECH Act, business associates and subcontractors were not subject to direct enforcement. Instead, their obligations arose solely under the contractual terms of an agreement commonly called the "Business Associate Agreement" (BAA). As such, business associates and subcontractors were only subject to contractual remedies for breach of the BAA. But, as a result of the HITECH Act, business associates and subcontractors are now subject to direct enforcement by the OCR, the DOJ and State Attorneys' General.

More importantly, however, covered entities are financially responsible for the HIPAA violations of their business associates, and business associates are financially responsible for the HIPAA violations committed by their subcontractors. HHS clarified these obligations in the Omnibus Rule:

A covered entity [or business associate, as applicable,] is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the covered entity [or business associate, as applicable], including a workforce member or business associate [or subcontractor, as applicable], acting within the scope of the agency.

As a result, covered entities and business associates have a strong interest in ensuring that those they engage to provide services can meet both the requirements of the HIPAA Rules as well as any indemnification provisions.

The civil penalty provisions are tiered, with the penalty amount increasing with the organization's level of knowledge regarding a particular violation (*i.e.*, culpability) and whether the violation was corrected in a timely fashion.

The HHS Secretary has a broad amount of discretion in imposing civil monetary penalties. However, HHS made clear in

Table 1. Tiered Penalty Structure[14]

Violation - § 1176(a)(1)	Each violation	All such violations of an identical provision in a calendar year
Did Not Know Did not know and, by exercising reasonable diligence, would not have known that the covered entity, business associate, or subcontractor violated a provision	$100–$50,000	$1.5 M
Reasonable Cause Violation was due to reasonable cause and not to willful neglect	$1,000–$50,000	$1.5 M
Willful Neglect – Corrected Violation that was due to willful neglect and was corrected during the 30-day period beginning on the first date the covered entity, business associate, or subcontractor liable for the penalty knew, *or, by exercising reasonable diligence, would have known* that the violation occurred	$10,000–$50,000	$1.5 M
Willful Neglect – Not Corrected Violation that was due to willful neglect and was *not* corrected during the 30-day period beginning on the first date the covered entity, business associate, or subcontractor liable for the penalty knew, *or, by exercising reasonable diligence, would have known* that the violation occurred	$50,000	$1.5 M

the Omnibus Rule that, "the Department will not impose the maximum penalty amount in all cases but will rather determine the amount of a penalty on a case-by-case basis, depending on the nature and extent of the violation and the nature and extent of the resulting harm, as required by the HITECH Act, as well as the other factors set forth at [45 C.F.R.] § 160.408."[15] These factors include, among other things, (1) the number of individuals affected by the breach, (2) whether the violation caused physical harm, (3) whether the violation resulted in financial harm, (4) whether the violation resulted in harm to an individual's reputation, (5) whether the current violation is the same or similar to previous indications of noncompliance, and (6) whether and to what extent the covered entity, business associate, or subcontractor has attempted to correct previous indications of noncompliance.[16]

Table 2. Summary of OCR Enforcement Actions

Entity Name	Penalty Amount	HIPAA Rules Violated	Brief Summary of Violation	Incident Date	Settlement Date
Cignet Health	**$4.3M**	Privacy Rule, $3M for willful neglect per HITECH	Denying patients access to medical records	Prior to 3/1/2009	2/4/2011 *(this was penalty; not a settlement)*
General Hospital Corp. & Physicians Org.	**$1M**	Privacy Rule	Left documents on subway	3/9/2009	2/14/2011
UCLA Health System	**$865,500**	Privacy & Security Rules	Workers snooping on celebrity patients	Prior to 6/5/2009	7/5/2011
Blue Cross Blue Shield of TN	**$1.5M**	Privacy & Security Rules	unencrypted hard drives stolen from a leased facility	Prior to 11/3/2009 (self reported)	3/13/2012
Phoenix Cardiac Surgery	**$100K**	Privacy & Security Rules	posting appt. on an online, publicly accessible calendar	Prior to 2/19/2009	4/11/2012
Alaska Dept. of Health & Human Services	**$1.7M**	Privacy & Security Rules	unencrypted portable media device stolen from car of employee	10/12/09 (self reported)	6/25/2012
Massachusetts Eye and Ear Infirmary	**$1.5M**	Privacy & Security Rules	theft of unencrypted personal laptop while at conference	Prior to 4/21/10 (self reported)	9/13/2012
Hospice of Northern Idaho	**$50K**	Security Rule	theft of unencrypted laptop	Prior to 2/16/11 (self reported)	12/17/2012
Idaho State University	**$400K**	Security Rule	disabled server firewall for ~ 10 mo. resulting in a breach	Prior to 8/9/2011 (self reported)	5/10/2013
Shasta Regional Medical Center -	**$275K**	Privacy Rule	senior leaders at co. met w/media to discuss medical services provided to a patient w/o a valid written authorization	1/4/2012 (read article in LA Times)	6/3/2013
WellPoint	**$1.7M**	Privacy & Security Rules	software update to web-based database left ePHI publicly accessible	Prior to 6/18/10 (self reported)	7/8/2013
Affinity Health Plan	**$1,215,780**	Privacy and Security Rules	returned copiers to a leasing agent w/o erasing the copier hard drives	Prior to 4/15/10 (self reported)	8/7/2013
Adult & Pediatric Dermatology	**$150K**	Privacy, Security, & Breach Notification Rules	theft of unencrypted personal thumb drive from employee vehicle	Prior to 10/7/11 (self reported)	12/24/2013
Skagit County, Washington	**$215K**	Privacy, Security, & Breach Notification Rules	moved money receipts containing PHI to a publicly accessible server	9/14 – 9/28, 2011 (self reported)	3/6/2014

A Few Enforcement Examples

The enactment of the HITECH Act has indeed led to increased enforcement by the Office of Civil Rights. Enforcement actions may arise as a result of a complaint filed with OCR, a news report, or a self-reported data breach. To date, OCR has taken action against fourteen different organizations, ranging from health plans, relatively small providers, a state agency and, most recently, a county government. These enforcement actions are briefly summarized in Table 2.

Additionally, a number of State Attorneys' General have taken action against covered entities with one taking action against a business associate. For example, the State Attorneys' General of Connecticut, Indiana, and Vermont have all take action against covered entities, with both Connecticut and Vermont taking action against Health Net[17] and Indiana taking action against WellPoint.[18] Notably, the Indiana Attorney General pursued an action against WellPoint under Indiana's data breach notification law because WellPoint failed to notify the State Attorney General's Office "without unreasonable delay."

Both the State Attorney General of Minnesota and the Federal Trade Commission took action against Accretive Health, a business associate, based on a data breach that happened in July 2011. Under the settlement with the Minnesota Attorney General, Accretive agreed to "cease all operations in Minnesota within ... 90 days, or by November 1, 2012. The company [will] then be subject to an outright ban on operating in Minnesota for two years, after which, for the next four years, it can only reenter the State if the Attorney General agrees to a Consent Order regarding its business practices in the State." [19]

In addition to the enforcement actions described above, there has also been an increase in plaintiffs' litigation stemming from healthcare related data breaches. There is no private right of action under HIPAA. As a result, these actions are typically filed under state law alleging negligence, intentional infliction of emotional distress, negligent entrustment, breach of confidentiality, invasion of privacy, and a number of other claims.[20] In general, plaintiffs' have experienced varied amounts of success because plaintiffs'

cannot demonstrate damages. With few exceptions, to prevail, plaintiffs' must be able to demonstrate that the data breach caused them some form of financial harm. To the extent plaintiffs' can demonstrate such harm, such as, for example, if they were victims of identity theft, then the cases become more difficult for defendants to overcome. Nonetheless, even if the defending organizations prevail, class action litigation is very costly.

What Should IT Vendors Do Now?

As a preliminary matter, data centers and other IT vendors should determine whether they are subject to HIPAA compliance. To do this, they should evaluate their existing customer base to find out: (1) whether any are healthcare providers, health plans or healthcare clearinghouses; and (2) if not, whether they provide services to entities that then provide services to these covered entities. Or, alternatively, vendors should find out whether they have executed any business associate agreements.

Vendors that are subject to HIPAA compliance, or have otherwise agreed they are by executing a BAA or a subcontractor associate agreement, must then evaluate their existing level of compliance. Generally, this is done by undertaking a Risk Analysis, which is a required element under the HIPAA Rules and a "foundational element in the process of achieving compliance."[21] In addition to the Risk Analysis, vendors should consider reviewing the OCR Audit Protocol and using that Protocol as an additional means of evaluating compliance.[22]

To the extent possible, IT vendors should draft their own form BAAs as opposed to executing form agreements provided to them by the covered entities or business associates, as appropriate. Generally, so-called 'standard' BAAs will not be appropriately limited to services provided by the IT vendors. This is particularly true for data centers, which do not have direct contact with patients. But, standard BAAs generally contain terms that require, for example, for the Business Associate to provide the patient access to his/her medical records. As HHS has made clear, "business associates are liable for providing electronic access in accordance with their business associate agreements."[23] To minimize risks, vendors should generally avoid agreeing to terms that are outside their scope of services.

Importantly, vendors must understand that these obligations cannot be ignored. HHS has made clear that responsibility for protecting PHI travels

with the PHI "no matter how far 'down the chain' the information flows."[24] Additionally, while covered entities, business associates, and subcontractors must enter into Business Associate Agreements, "direct liability under the HIPAA Rules [attaches] regardless of whether the [the parties] have entered into the required business associate agreements."[25]

Finally, vendors should carefully evaluate their level of risk and purchase cyberliability insurance in accordance with the level of risk they have accepted. According to a 2013 study on the global cost of a data breach, the cost to repair a data breach in 2012 was approximately $188 per record.[26] At that rate, the cost to repair a breach impacting 50,000 records is $9.4 million. Such costs may be prohibitive for a number of organizations. As such, vendors should appropriately limit their liability in contracts and avoid agreeing to unlimited liability in any transaction, unless they are prepared to go out of business for that specific deal.

REFERENCES

(1) Pub. L. 104-191, 110 Stat. 1936 [hereinafter HIPAA], available at http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/content-detail.html, was signed into law on August 21, 1996 by William Jefferson "Bill" Clinton.

(2) See id. at § 261, which indicates that the purpose of Title II of HIPAA is 'Administrative Simplification.'

(3) H.R. Rep. No. 104-496 Part 1 at 99 (1996), available at http://www.gpo.gov/fdsys/pkg/CRPT-104hrpt496/pdf/CRPT-104hrpt496-pt1.pdf.

(4) Public Law 111–5, 123 Stat. 115 [hereinafter the HITECH Act], available at http://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf.

(5) See Joshua D. W. Collins, Toothless HIPAA: Searching for a Private Right of Action to Remedy Privacy Rule Violations, 60 VANDERBILT LAW REV. 199 (2007).

(6) See e.g., Statement of Deven McGraw, Director, Health Privacy Project, Center for Democracy and Technology, S. Hrg. 111–213, Serial No. J–111–3 (Jan. 27, 2009) ("strong privacy protections must be part of any legislation that moves health IT").

(7) The HIPAA Rules were published in the Federal Register on January 25, 2013. See 78 FR 5566, available at http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

(8) See 45 C.F.R. § 160.103.

(9) See 45 C.F.R. § 160.103.

(10) 78 F.R. 5571 – 72 (Jan. 25, 2013).

(11) Id. at 5571.

(12) Id (emphasis added).

(13) Id. at 5572 (emphasis added).

(14) See 45 C.F.R. § 160.404.

(15) 78 F.R. 5583 (Jan. 25, 2013).

(16) 45 C.F.R. § 160.408.

(17) Press Release, Connecticut Office of the Attorney General, Attorney General Announces Health Net Settlement Involving Massive Security Breach Compromising Private Medical and Financial Info, http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=462754 (July 6, 2010); Press Release, Vermont Office of the Attorney General, Attorney General Settles Security Breach Allegations Against Health Insurer, http://www.atg.state.vt.us/news/attorney-general-settles-security-breach-allegations-against-health-insurer.php (Jan. 18, 2012).

(18) Press Release, Indiana Office of Attorney General, Attorney General Reaches Settlement with WellPoint in Consumer Data Breach, http://www.in.gov/portal/news_events/71252.htm (July 5, 2011).

(19) Press Release, Minnesota Attorney General, Attorney General Swanson Says Accretive Will Cease Operations in the State of Minnesota Under Settlement of Federal Lawsuit, Cannot Reenter Minnesota For Six Years Without Attorney General's Agreement, http://www.ag.state.mn.us/consumer/pressrelease/07312012accretiveceaseoperations.asp (July 31, 2012).

(20) See e.g., R.K. v. St. Mary's Medical Center, No. 11-0924 (Ct. of App. W.Va 2012).

(21) HHS, OCR, Guidance on Risk Analysis Requirements under the HIPAA Security Rule 2 (July 12, 2010), available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.

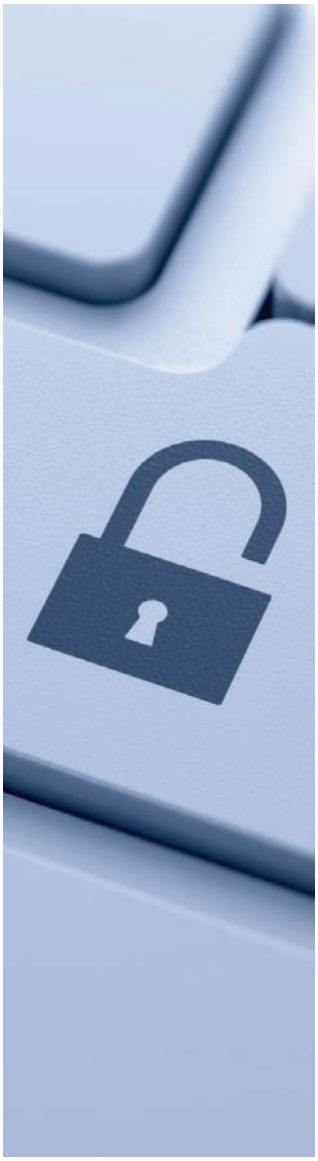
(22) HHS, Office for Civil Rights, Audit Program Protocol, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html (last visited Mar. 21, 2014) ("Please be aware that the protocol has not yet been updated to reflect the Omnibus Final Rule[.]")

(23) 78 FR 5599 (Jan. 25, 2013).

(24) 78 FR 5574 (Jan. 25, 2013).

(25) Id. at 5599.

(26) Ponemon Institute LLC, 2013 Cost of Data Breach Study: Global Analysis (May 2013), available at http://www.ponemon.org/library/2013-cost-of-data-breach-global-analysis.



Tatiana Melnik is an attorney focusing her practice on IT, data privacy and security, and regulatory compliance. She can be reached at tatiana@melniklegal.com