Microsoft

Think Cloud Compliance

Privacy and Security Compliance in the Health Care Cloud

Paul M. Schwartz,
Professor of Law,
Berkeley Law School

> “The cloud permits a health care organization to focus on its core competency in medicine and to allow computing companies to secure and operate their networked computing environment.”

One of the most dynamic areas of technology today is cloud computing. Our data is moving off our own devices and into different configurations of remotely managed servers. The market for these services is increasing by a double digit annual percentage rate. As Gartner explains, IT spending is moving from traditional hardware and software to cloud computing.[1] According to this research company, the shift in spending on the cloud will amount to $1 trillion over the next five years.

The cloud represents a new model for the deployment of computing resources by providing on-demand access to computing power. It allows computing to be purchased like a utility, such as electricity, instead of being provisioned internally. A shift to cloud technologies in health care offers great promise. These include increasing administrative efficiency, providing for the kinds of massive computing power that digital medicine requires, furthering patient-centric health care, and helping data-driven research. Moreover, use of the cloud can enhance privacy and security by permitting health care organizations to access expertise and investment in these areas without starting from scratch on their own. The cloud permits a health care organization to focus on its core competency in medicine and to allow computing companies to secure and operate their networked computing environment.

This Essay begins by discussing the rise of health care clouds and exploring the grounds for their increased adoption. It then turns to the law and explores the two goals of U.S. federal law regarding digital health care data. First, federal law has sought to promote the use of digital health care records and their electronic exchange. Second, it has established strong privacy and security requirements for the use of this information.

After tracing this history, this Essay explores the substance of these legal requirements. Federal law now provides detailed substantive requirements for personal health information. It regulates the use of personal health data by both “covered entities,” including traditional health care providers, and their “business associates,” namely, the vendors that they use. Guidance from the U.S. Department of Health & Human Services (HHS) makes it clear that cloud providers are business associates and directly fall under federal health care privacy and security law.[2] The law sets out the obligations that business associates must fulfill and requires “business associate agreements” (BAA’s) between covered entities and cloud providers.[3] In a nutshell, cloud providers are business associates, and they are the ones in the health care area with experience helping hundreds and sometimes thousands of companies move to the cloud. This experience helps them provide solutions that comply with the requirements of the Health Insurance Portability and Accountability Act (HIPAA).

The Rise of the Cloud and Regulation of Health Care Information

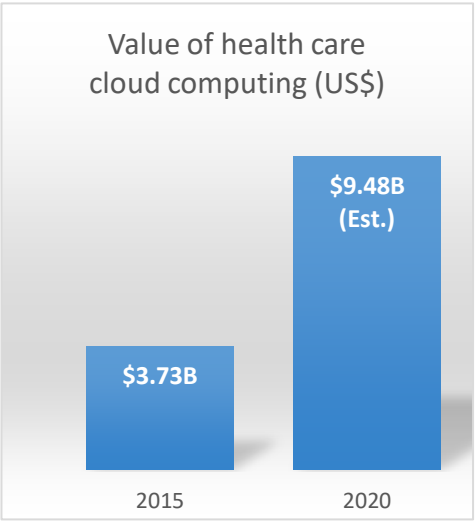
Health care clouds are now a significant factor in medicine. Their rise reflects their ability to fulfill a variety of needs in contemporary health care. This Part discusses the factors that have led to a rise of health care clouds. It will also analyze how federal law encourages use of digital health data and provides strong privacy and security protections for this information.

The Rise of Health Care Clouds

The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources . . . that can be rapidly provisioned and released with minimal management effort or service provider interaction."[4] The concept of the cloud is, thus, tied to the transferring of responsibilities from one party to another. The benefit of such an arrangement is that it permits new efficiencies in computing management. The NIST provides additional specification in defining cloud services. It identifies three general service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).[5] In SaaS, the end user relies on a provider's applications that run within the cloud. Clients access these applications through a client interface, such as a Web browser.

In PaaS, the provider delivers a development and deployment stack, in which the consumer receives integrated software for development and use. The consumer has control over the deployed applications. PaaS has been especially attractive for smaller healthcare Independent Software Vendors (ISV's). A significant trend has been for ISV's to move their tailored commercial solutions to the Cloud and to draw on the infrastructure of large, experienced cloud providers. That permits the ISV to focus on software solutions for integration of health care functions such as billing, records management, and mobile health data.

Finally in IaaS, the consumer can deploy and run software, including operating systems and applications. The customer of IaaS rents and uses external computing resources by paying for their use. In sum, the Cloud permits different functions and operations concerning data processing to be packed as modular units that can be pulled apart and reassembled.[6] The cloud provides new flexibility for companies in deciding on the shape and form of computing work.



Source: MarketsandMarkets

Health care organizations are now making increased use of the cloud. In 2015, the health care industry's need for cloud computing was estimated to be worth $3.73 billion annually.[7] By 2020, that number is predicted to reach $9.48 billion annually.[8] According to one analyst, "the tipping point is here."[9] Health care clouds offer SaaS, PaaS, and IaaS. There are also public and private clouds available for health care as well as hybrid service models. A public cloud is offered by a service provider to organizations and the general public. A private cloud is dedicated to a single organization. For health care entities, there are great potential benefits from the cloud, and different organizations have made use of different service models.

Five factors that have driven adoption of cloud-solutions for health care. First, the cloud provides a path to increase efficiency and lower administrative costs in health care. The recourse to the cloud permits an organization to purchase only the amount of computing resources that it requires. A medical provider can free up resources by only paying for computing resources they use as when it purchases services from a utility company.

Second, many aspects of health care are now digital. This process began in the 1990's with a shift to electronic insurance records. Today, digitalization sweeps in patient records and digital medical test results, including X-rays, MRI's, and CT scans. The storage and sharing of this information requires high capacity resources, such as those provided by cloud service providers. This approach permits health care entities to benefit from the massive economies of scale associated with large cloud centers. It allows them to "scale" up or down depending on their needs at different times.

Third, patient-centric medicine is furthered when digital resources are available for health care consumers. Interactions between patient and physicians can be improved by mobile devices, instant alerts, and digital health care reminders. A shift to the cloud can improve the treatment of patients as empowered partners in their health care.

Fourth, health care research now depends on Big Data, which requires significant computer resources. Already in 2009, the Institute of Medicine noted a shift from traditional clinical trials "in which patients volunteer to participate in studies to test the efficacy of new medical interventions."[10] Research was adopting an "information based" model that started with existing data and examining it for interesting correlations and patterns. Physicians and health care experts are now manipulating gigantic data sets, for which secure research platforms are essential.

Finally, the use of cloud services can enhance privacy and security. It does so by permitting a health care entity to focus on medicine and rely on a cloud provider to operate and secure its networked environment. In a sense, therefore, the question is less whether "to cloud or not to cloud," but rather whether to seek an external cloud provider or to attempt to build cloud capacity internally. In 2014, a survey of health care providers by the Health Information and Management Systems Society (HIMMS) found 83 percent of IT health care executives reported use of cloud services.[11] This survey also found that 67 percent of IT health care organizations were already running SaaS-based applications.

> "In 2014, a survey of health care providers by the Health Information and Management Systems Society (HIMMS) found 83 percent of IT health care executives reported use of cloud services."

Health care entities rank among the most highly regulated entities for privacy and security. To cut through the thicket of regulation, cloud services specializing in the health care market offer tailored solutions for different approaches to networked data solutions. As the Center for Democracy & Technology has noted of cloud service providers (CSPs): "CSPs can often provide a level of data security that health care providers could not achieve on their own."[12] It found the potential here particularly promising for "small health care providers."[13]

Cloud providers invest upfront in HIPAA-compliant technology and management solutions and are then able to spread these costs among all their customers. As an example, "[i]t can take hundreds of thousands of dollars to replace technology and processes that are not HIPAA compliant."[14] Cloud services can "build in" compliance with such requirements in their technology, and, in turn, permit health care entities to concentrate on providing health care and engaging in research.

This trend to adoption of cloud services by health care organizations has been shaped by two major legal developments: (1) the encouragement of the use of electronic data in health care; and (2) an increase in privacy and security regulation. The next section of this Essay examines these two aspects of the current health care landscape. It will then analyze the content of existing privacy and security law for health information. These regulations have paved the way to a cloud computing environment of shared legal responsibilities and clarity regarding each party's obligations.

Encouraging Use of Electronic Data, Protecting Privacy and Security

Health care regulation in the U.S. has sought to increase efficiencies and lower costs by promoting a transition from paper to electronic records. This process has been accompanied by a second one, namely, the enactment of increased safeguards for privacy and security standards. Within a relatively short time, the U.S. health care sector has moved into a digital universe and one with a tight web of legal obligations regarding personal data. Personal health information is now one of the most regulated kinds of data in the U.S.

The timeline begins in the early 1990's with a legal landscape for personal health information that was largely free of federal obligations. At that time, one analyst observed that "video rental records are afforded more federal protection than are medical records."[15] A report from the Congressional Office of Technology Assessment from 1993 concluded, "The present legal scheme does not provide consistent, comprehensive protection for privacy in health care information, whether it exists in a paper or computerized environment."[16] In the 1990's, many mental health professionals advised patients not to seek insurance reimbursement because their psychiatric records might no longer be private.[17] In this period, significant agreement existed regarding the insufficiency of medical privacy in the United States.

The tide began to turn with the enactment of HIPAA.[18] In 1996, Congress enacted HIPAA as a way of furthering "portable" health care insurance. This statute prevents employment-based health insurance plans from excluding pre-existing conditions for new employees.[19] By doing so, HIPAA seeks to stop "job lock," a phenomenon in which employees remain tied to positions because of uncertainty regarding health care insurance from future employers.

A second important legislative goal in HIPAA concerned efficient processing of health insurance claims. To reach this goal, the statute created a uniform, national set of transactions and code set standards for electronic insurance claims. By replacing hundreds of existing local and proprietary formats, HIPAA sought to save the health care industry billions of dollars in administrative costs. This creation of "transaction and code set" standards represented an essential step towards a digital health care. The standardization of transactions and code set standards permitted electronic data interchanges without human input. In this fashion, HIPAA transformed an outmoded and wasteful system of paper insurance claims into one of electronic claims processing.

At the time of enactment of HIPAA, Congress was also concerned with the impact on privacy and security from the greater electronic sharing of health care information. It set itself a deadline of 1999 to enact necessary legislation in this area.[20] Its inability to reach consensus by that date shifted responsibility to HHS. This agency then promulgated the current framework of health privacy regulations.[21] It issued its final privacy rules in 2000[22] and security rules in 2003.[23]

The next important development in this area occurred in 2009. At that time, Congress enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act.[24] Like HIPAA, the Act sought to encourage use of electronic health care records. It was part of the American Recovery and Reinvestment Act of 2009 (ARRA), an economic stimulus bill enacted during the economic crisis that had started the previous year. The HITECH Act offered health care providers a mixture of carrots and sticks for adopting electronic health records. It provided financial incentives until 2015 for health care providers who demonstrated "meaningful use" of electronic health records. Its incentives totaled $19.2 billion for adoption of digital technology. Starting in 2015, the Act provided the Centers for Medicare and Medicaid Services with the authority to levy penalties on health care providers who were unable to demonstrate such use of electronic health records. The penalties

HHS.gov
Health Information Privacy

The **Health Information Technology for Economic and Clinical Health (HITECH) Act**, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information.

took the form of reductions in the amount of federal Medicare reimbursements for non-compliant entity.

Like HIPAA, HITECH did not merely encourage digitization of health records. It also took action to safeguard the privacy and security of health care data. This Essay now will examine the substance of the HIPAA and HITECH safeguards. It explores the requirements for privacy and security that federal law places on health care organizations.

Privacy and Security Regulation for Covered Entities

Federal law provides detailed substantive requirements for personal health information. HIPAA's requirements broadly extend to "covered entities"; this legal term of art refers to organizations such as a health plan, a health care clearinghouse, and a health care provider who are engaged in transmitting health care information electronically for billing and payment purposes.[25] The data protected under HIPAA is termed "PHI," which stands for "protected health information."

Under the privacy regulations, covered entities must provide a notice of their privacy practices to patients.[26] HIPAA further provides that individuals have a right to access any protected PHI that is used in whole or in part to make decisions about them.[27] For all uses and disclosures of information beyond those used for treatment, payment, or health care operations, the covered entity must obtain the patient's authorization unless another exception in HIPAA applies.[28] With some limitations, a covered entity cannot use protected health information in marketing without authorization.[29]

HHS has also issued important security requirements for health care entities. A critical concept is that of "electronic protected health information" (ePHI), which is the centerpiece of the Security Rule.[30] The Security Rule requires covered entities to "protect against any reasonably anticipated threats or hazards to the security or integrity of [e-PHI]."[31] The overall touchstone for an organization is to "[i]mplement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level."[32]

As a critical addition to the regulatory framework, the HITECH Act in 2009 extended the privacy and security rules beyond a covered entity to a "business associate."[33] Under HIPAA, a business associate is "an entity or person, other than a member of the workforce of a covered entity, that performs functions or activities on behalf of ... a covered entity that involve creating, receiving, maintaining, or transmitting PHI."[34] The logic behind HITECH's extension to business associates is impeccable. As the HHS Office for Civil Rights (OCR) explains, "[m]ost health care providers and health plans do not carry out all of their health care activities and functions by themselves."[35] Hence, there is a need for privacy and security obligations to go beyond the covered entity; privacy and security regulations now follow protected health information as different professional entities transfer, store, and process it.

> "…privacy and security regulations now follow personal health information as different professional entities transfer, store, and process it."

A further aspect of the HITECH Act is to establish the first federal data breach notification requirement.[36] Pursuant to the statute, OCR has issued detailed data breach notification regulations.[37] In addition, it has issued guidance regarding technologies and methodologies for rendering protected health information unusable.[38] The HITECH Act also increased the penalties for violation of the HIPAA privacy and security regulations.[39] It also requires OCR to conduct audits of HIPAA compliance.[40]

Finally, HIPAA regulations create an institutional structure for health care privacy and security. Covered entities must designate a "privacy officer" and a "security officer."[41] These individuals are responsible for the implementation and development of the entity's policies and procedures for privacy and security.[42]

Both the Privacy and Security Rule require covered entities to have training programs and data protection procedures in place.[43] Enforcement of HIPAA regulations is by the OCR. In addition, state attorney generals can take enforcement actions against entities whose violations of HIPAA impact residents in their states.[44] Only a few federal privacy laws create such a shared federal-state enforcement system.

Health Care Data in the Cloud

Today, the initial requirements of HIPAA are accompanied by additional cloud-specific regulations. The result is a model of shared responsibility, and one in which using the cloud can make compliance easier. The key to this approach is the "business associate agreement," which is required between a health care organization and its cloud provider.

Business Associate Agreements and their Contents

U.S. law has encouraged health care organizations to use electronic records and established strong legal requirements for privacy and security. The OCR has also issued guidelines to help pave the way for successful use of the cloud in health care. The key to understanding the resulting relationship between health care entities and cloud providers is the "business associate agreement" (BAA). The OCR has made it clear that cloud providers generally are "business associates" of the health care entity and must set out their obligations in a mandatory BAA. The OCR also offers clarity on how cloud providers should meet their regulatory obligations.

A 2016 Guidance from the OCR makes clear that a cloud service provider working with a covered entity will typically be a business associate. The OCR states, "When a covered entity engages the services of a CSP to create, receive, maintain, or transmit ePHI . . ., *the CSP is a business associate* under HIPAA."[45] As a result, a covered entity must enter into a business associate agreement that covers the compliance requirements set forth in HIPAA with a cloud service provider that is performing activities or services for it. OCR has also stated that a BAA is needed even when a "no-view service" is involved.

A cloud service provider is contractually liable under the terms of the BAA. The cloud service provider is also directly responsible for compliance with HIPAA's privacy and security rules as well as the HITECH data breach notification rule.

At a general level, the HIPAA regulations set out elements that a BAA must contain, and the OCR has published sample business associate contracts.[46] More specifically, the 2016 OCR Cloud Guidance provides counsel regarding the contents of a BAA with a cloud provider. Such an agreement "establishes the permitted and required uses and disclosures of ePHI by the business associate performing activities or services for the covered entity or [further] business associate."[47] The BAA is to contractually require the business associate to safeguard ePHI through actions that include the implementation of the Security Rule.

Cloud providers also contract through Subcontractor BAA's with other business associates. This scenario occurs, for example, in the context of PaaS, when health care ISV's move billing systems and records management to the cloud. It is a considerable advantage for health care ISV's to draw on established cloud companies, who are experienced with the legal and technology basis for HIPAA compliance. For example, Microsoft has published guidance on how to build secure health care solutions in Azure.[48] In these cases, BAA's will bind three parties to a shared framework: the cloud provider, the health care ISV, and the health care entity who uses the ISV solution.

The No-View Service and BAA

A BAA is needed even when a so-called "no-view service" is involved. In some instances, a cloud service provider may maintain encrypted ePHI on behalf of a covered entity or another business associate without having access to the decryption key. The OCR has stated that even if a cloud service provider stores encrypted ePHI to which it lacks a key, it should be considered to be a business associate. The OCR reaches this result because encryption alone does not guarantee fulfillment of all the obligations of the Security Rule. The Security Rules mandates safeguarding the "confidentiality, integrity, and availability of . . . ePHI." Yet, encrypted data might be corrupted by malware and become unavailable during an emergency or disaster. In addition, as the OCR states, "[E]ncryption does not address other safeguards that are also important to maintaining confidentiality, such as administrative safeguards to analyze risks to the ePHI or physical safeguards for systems and servers that may house the ePHI."

For more information, see: ***Guidance on HIPAA & Cloud Computing***, Health & Human Services: Office for Civil Rights, https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

Leading cloud providers are now experienced with BAA's, and their contents can include provisions for disaster recovery, audit rights, security and privacy, and return of data. Each of these provisions deserves at least brief explanation. Disaster recovery for data, sometimes called "fail-safes," provide for preservation of information in case of an emergency or unexpected event, such as a fire, natural disaster or other unplanned contingency. The cloud can further disaster recovery by permitting co-location of information. In this approach, the cloud provider stores data in more than one location. Audit rights at a cloud provider are provided by an independent third party. Through outside audit rights, a health care organization can check on the cloud provider's fulfillment of legal and contractual requirements.

Regarding privacy interests, the business associate must fulfill the legal mandates of HIPAA and HITECH. These include making available PHI "as necessary for the covered entity to meets its obligations to provide individuals with their rights to access, amend, and receive an accounting of certain disclosures of PHI."[49] As for security, pursuant to the HIPAA Security Regulation, the business associate must take steps to reduce risk to a "reasonable and appropriate level."[50] Moreover, this Regulation calls for a flexibility of approach to permit a covered entity and business associates to "use any security measures that allow" the party "to reasonably and appropriately implement the standards and implementation specifications as specified in" the Security Regulation.[51] Both parties must carry out a risk assessment and use security protocols and tools to protect PHI.

HIPAA privacy regulations require return of data at the termination of a BAA. This action can take the form of return or destruction of data. The OCR standard form for a BAA calls for the business associate to retain "only that protected health information which is necessary for ... to continue its proper management and administration or to carry its legal responsibility."[52] The remaining information is to be returned or destroyed.

Finally, in addition to the BAA, it is typical to have additional contractual details expressed in a Service Level Agreement (SLA). The SLA provides details about specific business expectations between the cloud service provider and the covered entity. According to the OCR, the issues covered in a SLA can include system availability and reliability; back up and data recovery; security responsibility; and use, retention and disclosure limitations.[53]

Experienced health cloud providers have responded to this regulatory framework by providing BAA's tailored to meet HHS requirements. Their availability "ready-made" lowers the cost of contracting for cloud services. It also demonstrates how experienced cloud providers have invested in both technology and legal compliance services in specialized cloud areas, such as health care.

Large cloud providers, such as Microsoft, started out serving general needs of their customers in the cloud. Over time, these entities moved into specialized markets, such as health care, and invested in tailoring their cloud platforms for the additional expectations in these contexts for availability, privacy and security. As part of this adaption, large cloud providers offer cloud services designed to meet applicable legal requirements. Regarding the market for U.S. health care clouds, Microsoft provides a BAA that addresses the compliance requirements set forth in HIPAA that is available to its health care customers. It also provides the results of independent audits to document that it meets HIPAA security practices as recommended by OCR.[54]

"Microsoft provides a BAA that addresses the compliance requirements set forth in HIPAA that is available to its health care customers. It also provides the results of independent audits to document that it meets HIPAA security practices as recommended by OCR."

The Health Cloud Provider and the Covered Entity: The Shared Responsibility Model

Health care organizations are now buying cloud computing services because outsourcing these requirements is more efficient than their taking on these tasks internally. This development has been encouraged by the legal system setting a strong baseline of privacy and security for health care data. This legal model promotes shared responsibility between the health care entity and the cloud provider. At the end of the day, each party has responsibility for the privacy and security risks that it is best situated to manage.

This model can further lower compliance costs for a covered entity by permitting it to purchase compliance expertise. A covered entity can contract for cloud services confident that the law regulates a cloud provider both directly as a business associate and through the required BAA. Cloud providers can assist health care organizations by providing skilled legal and IT professionals, tailored legal solutions, as well as digital resources that are HIPAA compliant.

Instead of a health care IT department "going it alone," the covered entity can draw on "tried and true, repeated controls and technologies" from a cloud provider.[55] The benefit is that experienced cloud providers will have been tested, vetted and audited by other health care clients. In contrast, an internal IT department at a health care entity may have been subject to far less scrutiny. An internal IT department only has one client, after all, which is the corporate entity in which it sits.

Health care organizations must also continue to meet their own legal responsibilities. HIPAA regulates a covered entity regardless of whether or not it uses a cloud provider. Health care organization must have mechanisms in place to meet the requirements that law directly imposes on them. Their obligations include meeting the law's use restrictions on PHI, risk analysis, staff training, and the steps for reasonable security. Like any other service that it might draw on, the covered entity must fulfill its legal obligations in how it implements a cloud computing environment. As OCR states in its Cloud Guidance, the cloud provider "is not responsible for the compliance failures that are attributable solely to the actions or inactions of the customer, as determined by the facts and circumstances of the particular case."[56] The law does not permit these health care entities to outsource their ultimate responsibility to follow the law.

> "The history of HIPAA-enforcement demonstrates that working within a framework for shared responsibility with an experienced cloud provider represents the best step towards preventing legal mishaps."

The history of HIPAA-enforcement demonstrates that working within a framework for shared responsibility with an experienced cloud provider represents the best step towards preventing legal mishaps. A surprising number of HHS OCR enforcement actions follow upon a failure to take such basic steps as having a BAA agreement or carrying out a risk analysis.[57] Moreover, health care providers at the receiving end of large fines have made such mistakes as storing non-encrypted ePHI on a laptop that was later stolen.[58] A cloud provider working within a shared responsibility framework might have assisted these entities by recommending proper policies or even providing technology such as Group Policy to ensure the enforcement of proper data handling and protection across all connected devices.

Ultimately, the best practice model for health care entities and their cloud providers requires their working together to synchronize efforts for privacy and security. The BAA and SLA are the touchstone documents in this regard. Moreover, meaningful communication must take place among both sides so that each entity can manage their risks.

Conclusion

Health care organizations have turned to cloud because it has become more productive under many circumstances for them to purchase computing activity as a utility rather than organize it by themselves. In turn, federal lawmakers and regulators have established strong privacy and security standards for health care organizations and health care clouds. From today's vantage point, a critical move in the right direction was made in the HITECH Act's extension of HIPAA regulation to a covered entity's business associate. As amended by the HITECH Act, federal law creates legal protections for protected health information that follow the information as different entities make use of it. In tandem with its strong regulations for health care privacy and security, federal law has additional rules and recommendations for entities that use health information in the cloud.

In taking these steps, the law encourages use of cloud companies that offer efficient, safe options. Privacy and security compliance should now be part of a health care entity's decision-making calculus when it chooses its service providers. Health care organizations have a great incentive today to work with cloud companies that successfully specialize in privacy and security.

About Professor Paul M. Schwartz

This white paper was written by Professor Paul M. Schwartz for Microsoft.

Paul Schwartz is a leading international expert on information privacy law. He is the Jefferson E. Peyser Professor at UC Berkeley School of Law and a Director of the Berkeley Center for Law and Technology. Schwartz is also a Special Advisor at Paul Hastings, where he works in the Privacy and Data Security Practice.

For more information about Professor Schwartz, visit http://paulschwartz.net.

NOTES

[1] Charles Babcock, Gartner Sees $1 Trillion Shift in IT Spending to Cloud, InformationWeek (July 25, 2016), http://www.informationweek.com/cloud/infrastructure-as-a-service/gartner-sees-$1-trillion-shift-in-it-spending-to-cloud/d/d-id/1326372

[2] Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-3, § 13401, 123 Stat. 115, 226–79 (2009)

[3] 45 C.F.R. § 164.504(e)(2)(11)(A)-(I).

[4] *Cloud Computing*, U.S. DEP'T OF COMMERCE: NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/programs-projects/cloud-computing (last visited Apr. 19, 2017).

[5] Paul M. Schwartz, *Information Privacy in the Cloud*, 161 Penn. L.Rev. 1623, 1633 (2013).

[6] Id. at 1625-26.

[7] Karin Ratchinsky, *Cloud today and tomorrow*, Healthcare IT News (Jan. 8 2016), http://www.healthcareitnews.com/blog/cloud-today-and-tomorrow-why-hospitals-are-tripling-use-cloud-services

[8] Id.

[9] Karin Ratchinsky, *Why the healthcare industry's move to cloud computing is accelerating*, CloudTech (June 27, 2016), https://www.cloudcomputing-news.net/news/2016/jun/27/why-healthcare-industrys-move-cloud-computing-accelerating/

[10] Institute of Medicine, Beyond the HIPAA Privacy Rule 19 (2009).

[11] Lindsey Gilpin, The state of the Industry Cloud in the healthcare sector, ZDNet (April 1, 2015), http://www.zdnet.com/article/the-state-of-the-industry-cloud-in-the-healthcare-sector/

[12] CTR. FOR DEMOCRACY & TECH., FAQ: HIPAA AND "CLOUD COMPUTING" (v1.0) 2 (Aug. 7, 2013), https://www.cdt.org/files/pdfs/FAQ-HIPAAandCloud.pdf.

[13] *Id.*

[14] Joe Kelly, *Challenges in Law Firm HIPAA Compliance*, Law360 (Oct. 23, 2015).

[15] Sheri Alpert, *Smart Cards, Smarter Policy: Medical Records, Privacy, and Health Care Reform*, 23 Hastings Ctr. Rep. 13, 13 (1993).

[16] OFFICE OF TECH. ASSESSMENT, 103D CONG., PROTECTING PRIVACY IN COMPUTERIZED MEDICAL INFORMATION 13 (1993)

[17] *See* Gina Kolata, *When Patients' Records are Commodities for Sale*, N.Y. Times, Nov. 15 1995, at A1.

[18] Pub. L. No. 104–191, 110 Stat. 1936 (1996) (codified in scattered sections of 26, 29, & 42 U.S.C.)

[19] *See* 29 U.S.C. § 1181 (2011).

[20] *Id.* at § 264(c)(1).

[21] *Id.*

[22] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160–164).

[23] Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,334 (Feb. 20, 2003) (codified at C.F.R. pts. 160–164).

[24] Pub. L. No. 111-3, §§ 13001–13424, 123 Stat. 115, 226–79 (2009) (codified at 42 U.S.C.).

[25] 45 C.F.R. § 160.103.

[26] *Id.* § 164.520

[27] *Id.* § 164.524.

[28] *Id.* § 164.522.

[29] *Id.* § 164.508.

[30] 45 C.F.R. § 164.306(a)(2)

[31] 45 C.F.R. § 164.306(a)(2).

[32] *Id.* § 164.308(b).

[33] Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-3, § 13401, 123 Stat. 115, 226–79 (2009)

[34] *Guidance on HIPAA & Cloud Computing*, HEALTH & HUMAN SERVS.: OFFICE FOR CIVIL RIGHTS, https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html (last visited Apr. 19, 2017).

[35] *Business Associates*, HEALTH & HUMAN SERVS.: OFFICE FOR CIVIL RIGHTS (Apr. 3, 2003), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html?language=es.

[36] 45 C.F.R. § 13402.

[37] HIPAA Breach Notification Rule, 45 C.F.R. § 164.400-414.

[38] *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, HEALTH & HUMAN SERVS.: OFFICE FOR CIVIL RIGHTS, https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html (last visited Apr. 19, 2017).

[39] *Id.* § 13410(d).

[40] *Id.* § 13411.

[41] *See* 45 C.F.R. § 164.530(a)(1) (privacy official); § 164.308(a)(2) (security official).

[42] *See id.*

[43] *See id.* § 164.530(b)(1) (privacy training); § 164.308(a)(3)-(5) (security training).

[44] For an overview, see Daniel J. Solove & Paul M. Schwartz, Privacy Law Fundamentals 102-109 (2017).

[45] *Guidance on HIPAA & Cloud Computing*, *supra* note 43 (emphasis in original).

[46] *See Business Associate Contracts*, HEALTH & HUMAN SERVS.: OFFICE FOR CIVIL RIGHTS (Jan. 25, 2013), https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

[47] *Guidance on HIPAA & Cloud Computing*, *supra* note 43.

[48] Microsoft Azure, A practical guide to designing secure health care solutions in Azure (Jan. 7, 2017), at https://docs.microsoft.com/en-us/azure/security/security-health-care-solution

[49] *Guidance on HIPAA & Cloud Computing*, HEALTH & HUMAN SERVS.: OFFICE FOR CIVIL RIGHTS, https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html.

[50] 45 C.F.R. § 164.308(a)(1)(ii)(B).

[51] *Id.* § 164.306(b)(1).

[52] HHS. Business Associate Contracts: Sample Business Associate Agreement Provisions (Jan. 25, 2013), at https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

[53] *Guidance on HIPAA & Cloud Computing*, HEALTH & HUMAN SERVS.: OFFICE FOR CIVIL RIGHTS, https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html.

[54] Microsoft, HIPAA/HITECH Implementation Guidance for Microsoft Azure (Feb. 7, 2017), https://gallery.technet.microsoft.com/Azure-HIPAAHITECH-Act-1d27efb0; HIPAA/HITECH Act Implementation Guidance for Microsoft Office 365 and Microsoft Dynamics CRM Online.

[55] Elizabeth Snell, *Utilizing Cloud Computing for Stronger Healthcare Data Security*, HealthIT Security, http://healthitsecurity.com/features/utilizing-cloud-computing-for-stronger-healthcare-data-security

[56] *Guidance on HIPAA & Cloud Computing*, HEALTH & HUMAN SERVS.: OFFICE FOR CIVIL RIGHTS, https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html.

[57] For a summary of enforcement actions from the OCR of the HHS, see Daniel J. Solove & Paul M. Schwartz, Privacy Law Fundamentals 8-11 (2017).

[58] HHS, *$2.5 million settlement shows that not understanding HIPAA requirements creates risk* (April 24, 2017), https://www.hhs.gov/about/news/2017/04/24/2-5-million-settlement-shows-not-understanding-hipaa-requirements-creates-risk.html.