Transcending the Cloud

A Legal Guide to the Risks and Rewards of Cloud Computing

Health Care in the Cloud –
Think You Are Doing Fine on Cloud Nine?
Hey You! Think Again. Better Get Off of My Cloud

ReedSmith

reedsmith.com

Health Care in the Cloud – Think You Are Doing Fine on Cloud Nine? Hey, You! Think Again. Better Get Off of My Cloud.

Chapter Authors[1]

Vicky G. Gormanly, Associate – vgormanly@reedsmith.com

Joseph I. Rosenbaum, Partner – jrosenbaum@reedsmith.com

Introduction

The interest level in storing health records in digital format has grown rapidly with the lower cost and greater availability and reliability of interoperable storage mechanisms and devices. Health care providers like hospitals and health systems, physician practices, and health insurance companies are among those most likely to be considering a cloud-based solution for the storage of patient-related health information. While lower cost, ubiquitous 24/7 availability, and reliability are key drivers pushing health care providers and insurers to the cloud, a number of serious legal and regulatory issues should be considered before releasing sensitive patient data into the cloud. This article seeks to highlight some of those concerns and considerations.

An important first step for any health care provider considering retaining the services of a cloud services provider, and ultimately moving data, programs or processing capability to a cloud environment, is to determine precisely what services are contemplated to be used. Depending on the services that are involved, certain provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") will be implicated. This article will highlight areas of consideration for health care providers who are exploring the possibility of engaging the services of a cloud services provider and moving some or all of patients' health records or other sensitive medical information to a cloud.

The Basics of Health Information Privacy

HIPAA's goals, as stated in the statute's introductory text, are "to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes."[2] This multitude of aspirations gave rise to the Administrative Simplification Regulations (the "Regulations"), which set forth a system for handling health data.[3] The Regulations, which are lengthy and complex, include the Privacy Rule, the Security Rule and the Enforcement Rule.[4]

In 2009, HIPAA's requirements were augmented by the Health Information Technology for Economic and Clinical Health Act ("HITECH"),[5] which was adopted as part of the American Recovery and Reinvestment Act in 2009. Among other things, HITECH expands the scope of civil and criminal liability for violations of the Privacy and Security Rules, and increases civil monetary penalties applicable to a violation. Further complicating matters, many state legislatures have added a layer of state regulation to the federally mandated requirements. Because of the wide reach of HIPAA and the multitude of players subject to its provisions, health care providers who decide to use a cloud-based system to store and manipulate data must give due consideration to HIPAA and its implementing regulations.

Cloud Services Providers and HIPAA

HIPAA extends only to "protected health information" ("PHI"), which is "individually identifiable health information that is transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."[6] "Individually identifiable health

information" is "information, including demographic data, that is created or received by a health care provider, health plan, employer, or health care clearinghouse, and relates to: (i) the individual's past, present or future physical or mental health or condition; (ii) the provision of health care to that individual; or (iii) the past, present or future payment for the provision of health care to the individual and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual."[7]

By statute, two types of entities are subject to HIPAA—covered entities and business associates. A "covered entity" is a (i) health plan; (ii) health care clearinghouse; or (iii) health care provider who transmits any health information in an electronic form in connection with a transaction covered by HIPAA.[8] Therefore, unlike most health care providers, a cloud services provider would not likely be considered a "covered entity" under HIPAA.

However, what is not clear is whether, under what circumstances, and to what extent, a cloud services provider would be considered a business associate. Generally, a "business associate" is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides services to, a covered entity that involves the use or disclosure of individually identifiable health information.[9] HITECH expanded the definition of "business associate." In July 2010, the agency charged with enforcement of the Privacy and Security Rules, the Office for Civil Rights ("OCR"), issued a proposed rule implementing certain provisions of HITECH. The proposed rule modified the definition of "business associate" to include, to some degree, subcontractors who are merely "downstream entities."[10] Sanctions for HIPAA violations have been broadened accordingly; a violation of an applicable requirement by a downstream entity will leave that entity directly liable for civil penalties.

Business Associate Status

Under HIPAA, as modified by HITECH, business associates are, among other things, directly responsible for: (i) establishing administrative and technical safeguards applicable to PHI, including limiting access to facilities housing such information; (ii) designating a privacy officer; (iii) developing an information privacy and security plan; (iv) providing notice of privacy practices; and (v) providing accountings of disclosures, as well as notices of unauthorized uses or disclosures of information. Thus, it is crucial for health care providers to determine whether services contemplated by the use of a cloud services provider would give rise to a "business associate" relationship.

Generally, the Regulations require a covered entity to have a contract or other arrangement in place with its business associates, such that the business associate provides satisfactory assurances it will appropriately safeguard any and all PHI that it receives, creates, maintains, or transmits on behalf of the covered entity. In light of this requirement, covered entities and business associates frequently demand that any contractor who even remotely does or might come into contact with that covered entity's PHI, sign a business associate agreement. Cloud services providers are no exception to this general assertion.[11]

That said, whether the services provided by a cloud services provider render it a business associate is not always clear, and recently has developed into a topic of much debate.[12] A cloud services provider's status with respect to a health care provider may depend on the type and degree of services it provides. Business associate "functions or activities" can include claims-processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing of claims. To the extent a cloud services provider performs these services, it would appear that a business associate relationship exists.

In the proposed rule promulgated last July, the OCR advised that it considers persons or entities that *facilitate the transmission of data* to be business associates.[13] When a "downstream entity" contracts with a business associate, the parties must adhere to the Privacy and Security Rules to the extent that they require access to PHI.[14] Alternatively, "data transmission organizations that do not require access to protected health information on a routine basis would not be treated as business associates," nor are "entities that act as mere conduits for the transport of protected health information but do not access the information other than on a random or infrequent basis."[15]

Therefore, in order for a health care provider to determine what, if any, HIPAA implications exist with respect to its use of cloud-based services, a factual analysis must be performed of the precise services that are contemplated. Specifically, a health care provider needs to consider whether and to what degree a proposed cloud services provider will need to have access to PHI in order to provide its services. If access to PHI is required to perform the services, the form and format of the data must be examined (*e.g.*, if the data is de-identified, its use will not be restricted[16]). The unfortunate implication, therefore, is

that it is not possible to reach a broad or general conclusion that a cloud services provider will always or never be subject to HIPAA. What can be determined is whether a specific service, consisting of specific activities, with access or use of specific health or other medical records and information, is or is not subject to HIPAA.

The Health Care Industry and HIPAA Demands

The highly regulated health care industry broadly includes hospitals, skilled nursing and long-term care facilities, specialty and primary care physicians and other health care professionals, insurers, pharmacists, software services providers, and last, but certainly not least, patients. With the impetus of government-paid incentives to adopt and meaningfully use electronic health records ("EHRs"), the use and sheer volume of EHRs is rapidly increasing. In addition, patients are increasingly being given the opportunity to create a web-based personal health record.[17] It is inevitable that some of this data will be stored in the cloud.

When considering engaging the services of a cloud services provider, the health care provider must take into account several characteristics and requirements of electronic and/or personal health record systems, including (i) interoperability; (ii) security requirements; and (iii) storage, access and reporting needs, for internal management, audit and compliance purposes. HIPAA covered entities should explore and evaluate a potential services provider's understanding of, and ability to support, the covered entity's unique regulatory needs and obligations. These abilities range from the obvious—maintaining data in a secure manner (*e.g.*, by the use of encryption)—to the less obvious, such as providing the covered entity with the ability to parse out data so that it can meet reporting or notification requirements, and allow it to account for uses and disclosures of PHI.

Interoperability

If the desire by health care industry players to implement an EHR system has one overarching theme, it is the tremendous benefit of having the same information available across the full health care continuum—from primary care providers to specialists; from surgeons to pharmacies; from insurers to patients. To realize this benefit, EHRs and the systems in which they are stored must be interoperable[18]—in other words, the systems must be able to "talk" to each other and exchange information, preferably quickly, accurately and seamlessly. Balancing interoperability with privacy is, therefore, an important consideration for health care providers who will increasingly require cloud services providers to have the demonstrated capability to offer a storage system that is able to communicate and exchange data with other systems, without compromising data security, in compliance with all legal and regulatory requirements.

Security

HIPAA's Security Rule sets forth in specific detail requirements for the physical, technical and administrative safeguards for PHI that is stored electronically.[19] Examples of these requirements include imposing physical limitations on access to data, implementing physical safeguards for workstations[20] that access the data, and providing protection against threats or hazards to the security or integrity of the information. Health care providers should evaluate prospective cloud services providers in light of these requirements in order to determine whether the cloud services provider understands the requirements and will be able to comply.

Storage and Access

The manner in which data will be stored and accessed is another concern for health care providers. Under HIPAA, individuals have the right, with some limitation, to seek access to their information and to authorize its use and disclosure by others. Specifically, the Privacy Rule sets forth the manner in which use and disclosure of health information may be authorized. Because of these requirements, health care providers should ensure that a potential cloud services provider has a system in place that allows for personal authorization of access to information. Health care providers who transfer these authorizations to an electronic format need to be able to electronically associate an authorization with the particular data that a patient is seeking to share. Most importantly, health care providers must ensure that no other data is released other than that data specifically authorized.

Additionally, health care providers need the ability to keep track of these personal authorizations, as well as unauthorized disclosures of PHI.[21] The Privacy Rule, as amended by HITECH, requires covered entities to make available, upon the request of an individual, an accounting of certain disclosures, including unauthorized disclosures, of the individual's PHI through an "electronic health record."[22] The individual has a right to request an accounting of disclosures that occurred during the three years prior to the request.[23] The type of data to be presented in such an accounting is set forth in the Privacy Rule. Although the regulatory interpretation of the manner in which electronic data is to be collected and presented is in flux, health care providers need to confirm that they will have the ability to access this data in a particular format. In

light of the potential for future changes, a cloud-based system should be as flexible as possible.

Conclusion

Cloud computing presents a huge potential for hospitals, health systems, physicians and even health insurers to obtain and maintain cost-effective EHRs. Indeed, cloud computing, if implemented in accordance with legal and regulatory requirements, can help assure that the patient is able to receive high quality health and medical care by correspondingly assuring that those responsible for the delivery and application of that care have timely, accurate and complete information, protected from alteration or file record corruption, and protected from inappropriate or improper disclosure. Web-based applications have many attractive and powerful features that allow for a productive exchange of health information and, consequently, better care for patients across the continuum of services. As this article and our experience have shown, numerous important legal and regulatory implications are related to the use of EHR, the storage of PHI and the "digitization" of health and medical information. Health care providers subject to HIPAA should give great attention to these implications, and carefully consider the risks associated with using cloud-based services for the operation and delivery of health and medical services.

— Biographies of Authors —

Vicky G. Gormanly, Associate – Washington, D.C. +1 202 414 9277 · vgormanly@reedsmith.com

Vicky is an associate in the Life Sciences Health Industry Group in the Washington, D.C., office. With a practice focused on health care regulatory compliance matters, Vicky supports the needs of a variety of health industry clients. She represents health care providers, suppliers, and pharmaceutical companies, on a broad range of complex regulatory issues (for example, Medicaid Drug Rebate Program, 340B, Tricare, State Pharmaceutical Assistance Programs, State Supplemental Rebate Programs, Medicare and Medicaid reimbursement, Anti-Kickback Statute, HIPAA). Vicky also counsels clients involved in the negotiation of rebate agreements between pharmaceutical manufacturers and pharmacy benefit managers, managed care companies, and group purchasing agreements.

Joseph I. Rosenbaum, Partner and Chair, Advertising Technology & Media Law Group
New York · +1 212 702 1303 · jrosenbaum@reedsmith.com
Blog: www.LegalBytes.com

Joe chairs Reed Smith's global Advertising Technology & Media Law practice, and has more than 30 years of international experience across a wide range of sophisticated and complex commercial transactions, in industries including advertising, entertainment and media, financial services, travel-related services, technology and many more. Joe specializes in the law and policy arising at the intersection of technology and online and behavioral advertising, social media, entertainment, finance, e-commerce, information security and digital rights, online gaming, promotions, privacy and data protection, among others. Joe's experience includes virtual worlds, mobile marketing, digital payments and PCI compliance, digital broadcasting, co-branded credit and gift cards, loyalty rewards programs, branded entertainment, online product placement and endorsements, user-generated content, buzz, word-of-mouth and viral marketing, licensing, software development and outsourcing. Joe lectures and writes extensively and, among others, has authored a book on outsourcing (*Outsourcing Agreements Line by Line*; Aspatore Publishing, 2004) and a seminal law journal article on privacy ("Privacy on the Internet: Whose Information Is It Anyway?"; *Jurimetrics Law Journal*, 1998). Joe's work has been cited by appellate courts, law reviews and journals, industry and trade periodicals. Joe is regularly quoted in widely respected publications such as the *National Law Journal*, Advertising Age, the American Banker, Euromoney and has been interviewed and appeared as a commentator on CNBC's *Squawkbox* and CNN Financial's *Business Unusual*. Joe is General Counsel & Secretary to the Interactive Advertising Bureau and a member of the Advisory Board of the Center for Law, Science and Technology at the Sandra Day O'Connor College of Law at ASU.

— Cloud Computing Task Force Leader —

Joseph I. Rosenbaum, Partner and Chair, Advertising Technology & Media Law Group
New York · +1 212 702 1303 · jrosenbaum@reedsmith.com
Blog: www.LegalBytes.com

Joe is a member of Reed Smith's global Advertising Technology & Media Law practice, and has more than 30 years of international experience across a wide range of sophisticated and complex commercial transactions, in industries including advertising, entertainment and media, financial services, travel-related services, technology and many more. Joe specializes in the law and policy arising at the intersection of technology and online and behavioral advertising, social media, entertainment, finance, e-commerce, information security and digital rights, online gaming, promotions, privacy and data protection, among others. Joe's experience includes virtual worlds, mobile marketing, digital payments and PCI compliance, digital broadcasting, co-branded credit and gift cards, loyalty rewards programs, branded entertainment, online product placement and endorsements, user-generated content, buzz, word-of-mouth and viral marketing, licensing, software development and outsourcing. Joe lectures and writes extensively and, among others, has authored a book on outsourcing (*Outsourcing Agreements Line by Line*; Aspatore Publishing, 2004) and a seminal law journal article on privacy ("Privacy on the Internet: Whose Information Is It Anyway?"; *Jurimetrics Law Journal*, 1998). Joe's work has been cited by appellate courts, law reviews and journals, industry and trade periodicals. Joe is regularly quoted in widely respected publications such as the *National Law Journal*, Advertising Age, the American Banker, Euromoney and has been interviewed and appeared as a commentator on CNBC's *Squawkbox* and CNN Financial's *Business Unusual*. Joe is General Counsel & Secretary to the Interactive Advertising Bureau and a member of the Advisory Board of the Center for Law, Science and Technology at the Sandra Day O'Connor College of Law at ASU.

— Endnotes —

1 The authors would like to thank Jackie Penrod for her contributions and assistance with this article.

2 Pub. L. 104-191.

3 The Administrative Simplification Regulations were developed to, among other things: (i) establish standards for electronic health transactions (*e.g.*, claims, enrollment, eligibility, payment, coordination of benefits); (ii) address the security of electronic health information systems; and (iii) establish privacy standards for health information.

4 45 C.F.R. §§ 160, 162, 164.

5 Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (Feb. 17, 2009). HITECH amended HIPAA with "improved privacy provisions and security provisions." Additionally, HITECH establishes incentive programs and other systems to encourage adoption and use of electronic and personal health records.

6 45 C.F.R. § 160.103.

7 *Id.*

8 *Id.*

9 *See id.*

10 *See* 75 Fed. Reg. 40,873 (July 14, 2010).

11 *See* Law Librarian Blog: Privacy and Data Security Risks in Cloud Computing (Feb. 10, 2010) ("any HIPAA covered entity would first have to negotiate and enter into a business associate agreement with a cloud provider before it could store records in a cloud computing facility"), available at http://lawprofessors.typepad.com/law_librarian_blog/2010/02/privacy-and-data-security-risks-in-cloud-computing.html. This advice, however, presumes that all cloud services providers will be considered business associates.

12 Multiple articles, blogs, and postings available on the Internet reveal uncertainty and debate among the various stakeholders and industry professionals as to whether cloud services providers act as business associates.

13 75 Fed. Reg. 40,872-40,873. (July 14, 2010). (Emphasis added).

14 *Id.* As an example of a "downstream entity" relationship, the proposed rule states that if a business associate contracts with a company to handle document and media shredding to securely dispose of paper and electronic PHI, the subcontractor would be directly required to comply with the applicable requirements of the Security and Privacy Rules in conducting its work.

15 75 Fed. Reg. 40,873 (July 14, 2010).

16 *See* 45 C.F.R. §§ 164.502(d); HITECH Act at Section 13401. De-identified health information is that which neither identifies nor provides a reasonable basis to identify an individual. 45 C.F.R. § 164.502(d)(2), 164.514(a), (b).

17 Companies that provide personal health records are not necessarily covered entities or business associates. However, the provisions of HITECH apply certain elements of HIPAA to personal health record services providers. Section 13407, HITECH.

18 Interoperability is also one of the requirements that an EHR services provider must demonstrate in order to become a certified provider. *See generally* www.healthit.hhs.gov (discussing certification of services provider programs).

19 45 C.F.R. §§ 164.105, 164.302-164.318. The Security Rule applies to "electronic protected health information that is created, received, maintained or transmitted by or on behalf of the health care component of the covered entity."

20 A "workstation" is "an electronic computing device, for example, a laptop or desktop computer or any other device that performs similar functions, and electronic media stored in its immediate environment." 45 C.F.R. § 164.304.

21 Under certain circumstances, PHI may be shared without first obtaining an authorization from the patient. *See* 45 C.F.R. § 164.512.

22 HITECH defines "electronic health record" as "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff."

23 Section 13405(c)(1)(B), HITECH.