Cloud Computing, Part Three: Health Care in the Cloud–Think You are Doing Fine on Cloud Nine? Think Again. Better Get Off of My Cloud

By Joseph I. Rosenbaum and Nancy E. Bonifant

Joseph I. Rosenbaum is a Partner, and the Chair of the Advertising Technology & Media Law Group in the New York office of Reed Smith. He 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 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 L.J., 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, and 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.

Nancy E. Bonifant is an Associate in the Washington, D.C. office of Reed Smith. She is a member of the Life Sciences Health Industry Group, practicing in the area of health care regulatory law. Nancy works with all types of health industry clients, including acute and post-acute institutional providers, medical device and pharmaceutical manufacturers, pharmacies, independent diagnostic testing facilities, DMEPOS suppliers, and hospice programs. Her practice focuses on fraud and abuse compliance (for example, compliance with the Federal Anti-Kickback Statute, the Stark Law, and beneficiary inducement prohibition), False Claims Act defense, government investigations, and Medicare reimbursement. Nancy also counsels health care providers and their vendors on health information privacy and security compliance (HIPAA and state law), assisting them in negotiating their BAAs, developing and implementing HIPAA/HITECH compliance programs, and addressing various aspects of HIPAA-related exposure, including breaches, and issues concerning the sale of PHI and marketing considerations, as well as ensuring that corporate transactions involving PHI appropriately address the parties' respective HIPAA obligations.

I. Introduction

The level of interest 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. With this has come increased interest in cloud computing.[1] Health care providers, including hospitals and health systems, physician practices, and health insurance companies, are among those likely to be considering a cloud-based solution for the storage of patient-related health information. While lower cost, ubiquitous 24/7 availability,[2] 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.[3] This article highlights 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

1. *See, e.g.*: Joseph I. Rosenbaum & Keri S. Bruce, *Cloud Computing, Part Two: Advertising and Marketing—Looking for the Silver Lining, Making Rain*, 65 Consumer Fin. L.Q. Rep. 431 (2011); Don Clark, *Cloud-Computing Firm Workday's IPO Soars*, Wall Str. J., Oct. 13-14, 2012, at 83.

2. Twenty-four hours per day, seven days per week.

3. *See, e.g.*, Adam W. Snukal, Joseph I. Rosenbaum & Leonard A. Bernstein, *Cloud Computing—Transcending the Cloud: A Legal Guide to the Risks and Rewards of Cloud Computing, Part One*, 65 Consumer Fin. L.Q. Rep. 57 (2011).

the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[4] will be implicated. This article focuses on 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 their patients' health records or other sensitive medical information to a cloud computing environment.

II. 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."[5] This multitude of aspirations gave rise to the HIPAA Regulations, which set forth a system for handling health data.[6] The HIPAA Regulations, which are lengthy and complex, originally included the Privacy Rule,[7] the Security Rule,[8] and the Enforcement Rule.[9]

In 2009, HIPAA's requirements were augmented by the Health Information Technology for Economic and Clinical Health Act (HITECH),[10] which was adopted as part of the American Recovery and Reinvestment Act of 2009. Among other things, HITECH expanded the scope of civil and criminal liability for violations of the Privacy and Security Rules, increased the civil monetary penalties applicable to a violation,[11] and established the foundation for the Breach Notification Rule.[12]

On January 25, 2013, the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services published the long-awaited HITECH Omnibus Final Rule, which amended significant portions of the HIPAA Regulations and finalized the Breach Notification Rule.[13] In particular, the HITECH Omnibus Final Rule extended to business associates of health care providers (discussed further below) the requirement to comply directly with the Security Rule and significant aspects of the Privacy Rule.[14]

Further complicating matters, many state legislatures have added a layer of state regulation to the federally-mandated requirements.[15] Because of the wide reach of HIPAA and HITECH, and the multitude of players subject to their provisions, health care providers who decide to use a cloud-based system to store and manipulate data must give due consideration to HIPAA and HITECH and their implementing regulations.

III. 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."[16] "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: (1) the individual's past, present or future physical or mental health or condition; (2) the provision of health care to that individual; or (3) the past, present or future payment for the provision of health care to the individual and that

4. Pub. L. No. 104-191, 110 Stat. 2033 (1996) (codified at 26 U.S.C.A. §§ 98900 *et seq*. (2011 & 2012 Suppl.)). *See also* the Health Information Technology for Economic and Clinical Health Act, Tit. XIII of Division A & Tit. IV of Division B of the American Recovery and Investment Act of 2009, Pub. L. No. 111-5, 123 Stat. 258 (2009). *See also infra* notes 5 - 8. The implementing regulations are codified primarily at 45 CFR pts. 160 - 164. *See*, *e.g.*, 45 CFR pt. 160 and 164, subpts. A and E (the Privacy Rule) and discussion below.

5. *See supra* note 4. *See generally* Anne Wallace, *The Impact of HIPAA on Financial Institutions*, 56 Consumer Fin. L.Q. Rep. 231 (2002).

6. *See* 45 CFR pts. 160, 162 & 164 (as amended through Mar. 23, 2013) [HIPPA Regulations]. The HIPAA Regulations were developed to, among other things: (1) establish standards for electronic health transactions (*e.g.*, claims, enrollment, eligibility, payment, coordination of benefits); (2) address the security of electronic health information systems; and (3) establish privacy standards for health information. *Id*. *See also* U.S. Dept. of Health & Human Services, Health Information Privacy, HIPPA Administrative Simplification Statute and Rules, *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html (last visited Sept. 23, 2013).

7. *See* HIPAA Regulations, *supra* note 6, 45 CFR pts. 160 & 164, subpts. A & E.

8. *See* HIPAA Regulations, *supra* note 6, 45 CFR pt. 164, subpts. A & C.

9. *See* HIPAA Regulations, *supra* note 6, 45 CFR pt. 160, subpts. C - E.

10. 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, 123 Stat. 258 (Feb. 17, 2009) [HITECH]. 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. *Id*.

11. *Id*.

    Section 13410(d) of the HITECH Act, which became effective on February 18, 2009, revised section 1176(a) of the Social Security Act (the Act) by establishing:

    - four categories of violations that reflect increasing levels of culpability;
    - four corresponding tiers of penalty amounts that significantly increase the minimum penalty amount for each violation; and
    - a maximum penalty amount of $1.5 million for all violations of an identical provision.

    It also amended section 1176(b) of the Act by:

    - striking the previous bar on the imposition of penalties if the covered entity did not know and with the exercise of reasonable diligence would not have known of the violation (such violations are now punishable under the lowest tier of penalties); and
    - providing a prohibition on the imposition of penalties for any violation that is corrected within a 30-day time period, as long as the violation was not due to willful neglect.

    See http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html.

12. *See* HIPAA Regulations, *supra* note 6, 45 CFR §§ 164.401 *et seq*.; *see also* Breach Notification for Unsecured Protected Health Information Interim Final Rule, 74 Fed. Reg. 42740 (Aug. 24, 2009).

13. *See* Modifications to the HIPAA Privacy, Security Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013) [HITECH Omnibus Final Rule].

14. *Id*. at 5598 - 99, 5601.

15. *See, e.g.*: Cal. Civ. Code §§ 56 *et seq*. (Confidentiality of Medical Information Act); Tex. Health & Safety Code Ann. §§ 181 *et seq*. (state law provisions governing medical records privacy).

16. HIPAA Regulations, *supra* note 6, 45 CFR § 160.103 (defining "protected health information").

identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual."[17]

Under the statute, two types of entities are subject to HIPAA--covered entities and business associates. A "covered entity" is a: (1) health plan; (2) health care clearinghouse; or (3) health care provider who transmits any health information in an electronic form in connection with a transaction covered by HIPAA.[18] Therefore, unlike most health care providers, a cloud services provider would most likely not be considered a "covered entity" under HIPAA.

However, the recent HITECH Omnibus Final Rule makes clear that if a cloud services provider *maintains* PHI (regardless of whether that PHI is actually *accessed* by the cloud services provider) on behalf of a covered entity, the cloud services provider would be considered a business associate and therefore now directly regulated under the HIPAA Regulations.[19]

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.[20] HITECH expanded the definition of "business associate." In both the preamble to the HITECH Omnibus Final Rule and the definition of "business associate," OCR clarifies that "an entity that maintains protected health information on behalf of a covered entity is a business associate…even if the entity does not actually view the protected health information."[21]

For example, according to OCR, "a data storage company that has access to protected health information (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.[22] Additionally, the HITECH Omnibus Final Rule modifies the definition of "business associate" to include "subcontractors" who are merely downstream entities if the subcontractor "creates, receives, maintains, or transmits protected health information on behalf of the business associate."[23] Sanctions for HIPAA violations have been broadened accordingly; therefore, a violation of an applicable requirement by a subcontractor will leave that entity directly liable for civil penalties.[24]

IV. Direct Liability and Business Associate Status

Before HITECH and the HITECH Omnibus Final Rule, the HIPAA Regulations did not directly apply to business associates. Instead, business associates' obligations were limited to contractual obligations. Specifically, the HIPAA Regulations required a covered entity to have a contract or other arrangement in place with its business associates (commonly referred to as a business associate agreement), such that the business associate provided satisfactory assurances that it would appropriately safeguard any and all PHI that it received or created on behalf of the covered entity.[25]

Now, under the HIPAA Regulations, as modified by the HITECH Omnibus Final Rule, business associates (and their subcontractors) are *directly* liable for civil monetary penalties under the Privacy Rule for "impermissible uses and disclosures of PHI," as well as the following requirements established by HITECH: (1) failing to provide breach notification to the applicable covered entity; (2) failing to provide access to a copy of electronic PHI to either the applicable covered entity, the individual, or the individual's designee (whichever is specified in the business associate agreement); (3) failing to disclose PHI where required by the Secretary of HHS to investigate or determine the business associate's compliance with the HIPAA Regulations; (4) failing to provide an accounting of disclosures of PHI, and (5) failing to comply with the requirements of the Security Rule with respect to electronic PHI.[26]

While "impermissible uses and disclosures of PHI" include any use or disclosure that would violate the Privacy Rule if done by a covered entity, OCR makes clear in the HITECH Omnibus Final Rule that it is the business associate agreements that "clarify and limit, as appropriate, the permissible uses and disclosures" of PHI by business associates. Therefore, the HITECH Omnibus Final Rule ties much of business associates' *direct* "liability to making uses and disclosures in accordance with the uses and disclosures laid out in such agreements, rather than liability for compliance with the Privacy Rule generally."[27]

That being said, direct liability is not dependent upon the actual existence of a business associate agreement--"liability for impermissible uses and disclosures attaches immediately when a person creates, receives, maintains, or transmits protected health information on behalf of a covered entity or business associate [in the case of a subcontractor] and otherwise meets the definition of a business associate."[28] Thus, in light of the current regulatory framework, it is critical for both health care providers and their vendors to determine whether the services contemplated by a proposed arrangement would give rise to a "business associate" relationship. Cloud services providers are no exception.

17. *Id.* (defining "individually identifiable health information").

18. *Id.*

19. *See* HITECH Omnibus Final Rule, *supra* note 13, at 5572, 5598 - 99 & 5601; *see also* HIPAA Regulations, *supra* note 6, 45 CFR § 160.103.

20. HIPAA Regulations, *supra* note 6, 45 CFR § 160.103 (defining "business associate").

21. *See* HITECH Omnibus Final Rule, *supra* note 13, at 5572.

22. *Id.*

23. *Id.* at 5572 - 5574; *see also* HIPAA Regulations, *supra* note 6, 45 CFR § 160.103 (defining "subcontractor").

24. *Id.*

25. HIPAA Regulations, *supra* note 6, 45 CFR § 164.502(e)(1)(i) (2012).

26. *See* HITECH Omnibus Final Rule, *supra* note 13 at 5598 - 99, 5601.

27. *Id.* at 5601.

28. *Id.* at 5598.

Prior to release of the HITECH Omnibus Final Rule, it was a topic of much debate whether the services provided by a cloud services provider rendered it a business associate.[29] Generally, it was thought that a cloud services provider's status with respect to a health care provider would depend on the type and degree of services it provided. To the extent cloud services providers performed business associate "functions or activities," including, for example: claims-processing or administration; data analysis; processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing of claims, it appeared that a business associate relationship would exist.[30]

By contrast, where the functions or activities to be provided by the cloud services provided would not require access to PHI, it appeared that a business associate relationship would not exist. For example, in the proposed rule issued in July 2010,[31] OCR advised that, under HITECH, persons or entities that facilitate the transmission of data and "require access to protected health information on a routine basis" would be business associates.[32] 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 would "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."[33]

In the HITECH Omnibus Final Rule, however, OCR significantly expanded the definition of business associate by distinguishing between vendors who provide data transmission services and only require access to PHI on a random or infrequent basis (the conduit exception) and vendors who *maintain* PHI on behalf of health care providers regardless of whether the PHI is actually accessed on a routine or infrequent basis.[34] According to OCR, while "mere conduits" that require random or infrequent access to PHI will not be considered business associates, vendors that maintain or store PHI, regardless of any access, will be considered business associates because of the "transient versus persistent nature of that opportunity."[35]

Therefore, in order for a health care provider or a cloud services provider to determine what, if any, HIPAA implications exist with respect to a proposed business arrangement, a factual analysis should be performed to determine whether the cloud services provider will maintain PHI on behalf of the health care provider in order to provide its services. If maintenance of any PHI is required in order to perform the services, then a business associate relationship exists

V. 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.[36] It is inevitable that some of this data will be stored and maintained in the cloud.

When considering engaging the services of a cloud services provider, the health care provider should take into account several characteristics and requirements of electronic and/or personal health record systems, including: (1) interoperability; (2) security requirements; and (3) 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, as well as the services provider's resulting regulatory obligations should a business associate relationship arise.

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. Importantly, to the extent cloud services providers are business associates, some of these abilities will also be regulatory obligations of the cloud services providers.[37]

VI. 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, *e.g.*: from primary care providers to specialists; from surgeons to pharmacies; and from insurers to patients. To realize this benefit, EHRs and the systems in which they are stored must be interoperable[38]--in other

29. *See, e.g.*, 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.

30. *See* HIPAA Regulations, *supra* note 6 , 45 CFR § 160.103.

31. *See* Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40868 (July 14, 2010) [HITECH Proposed Rule].

32. *Id.* at 40872 - 73.

33. *Id.* at 40873.

34 *See* HITECH Omnibus Final Rule, *supra* note 13, at 5571 - 72.

35. *Id.* at 5572.

36. Companies that provide personal health records are not necessarily covered entities or business associates. To the extent a *(Continued in next column)*

36. *(Continued from previous column)*

company offers personal health records to individuals on behalf of a covered entity, that service would give rise to a business associate relationship. *See* HITECH Omnibus Final Rule, *supra* note 13, at 5572.

37. *See supra* notes 26 - 28 and accompanying text.

38. Interoperability is also one of the requirements that an EHR services provider must demonstrate in order to become a certi- *(Continued on next page)*

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.[39]

VII. Security

HIPAA's Security Rule sets forth in specific detail the requirements for the physical, technical and administrative safeguards for PHI that is stored electronically.[40] Examples of these requirements include: imposing physical limitations on access to data; implementing physical safeguards for workstations[41] 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.

VIII. 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;[42] request an amendment to their information;[43] obtain an accounting of certain disclosures;[44] allow for certain uses and disclosures only with the individual's valid authorization;[45] and request certain restrictions on the use and disclosure of information.[46] For example, under the Privacy Rule, as modified by the HITECH Omnibus Final Rule, individuals now have the right to request certain restrictions of the use and disclosure of their PHI that covered entities are *required to comply with*. More specifically, where an individual requests to restrict disclosures to a health plan and (1) the disclosure is for payment or health care operations purposes and is not otherwise required by law and (2) the PHI pertains solely to health care services or items for which the individual, or another person on the individual's behalf (other than a health plan), has paid the covered entity in full, the covered entity must comply with the request.[47] Because of these requirements, health care providers should ensure that a potential cloud services provider has a system in place that allows for access to information and the ability to identify certain information that is subject to a required restriction.

Additionally, health care providers need the ability to keep track of certain disclosures of PHI, as well as unauthorized disclosures of PHI.[48] The existing Privacy Rule 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 maintained in a "designated record set" (*i.e.*, a health record).[49] The individual has a right to request an accounting of the disclosures that occurred during the six years prior to the request.[50] Importantly, while this requirement does not currently extend to disclosures of PHI for treatment, payment or health care operations purposes, this particular requirement under the Privacy Rule remains in flux even after release of the HITECH Omnibus Final Rule. Moreover, HITECH requires significant amendments to this requirement, and those amendments have yet to be implemented.

For example, HITECH removed the accounting exemption for disclosures to carry out treatment, payment, and health care operations through an electronic health record, but limits the individual's right to disclosures occurring during the three years prior to the request.[51] Although these regulatory obligations remain in flux, health care providers need to confirm that they will have the ability to access this data. In light of the potential for future changes, a cloud-based system should be as flexible as possible.

IX. Conclusion

Cloud computing presents significant potential benefits for hospitals, health systems, physicians and even health insurers in terms of obtaining and maintaining 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 higher 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. Thus, web-based applications have many attractive and powerful features that allow for a productive exchange of health information

38. *(Continued from previous page)*

fied provider. *See generally* www.healthit.hhs.gov (discussing certification of services provider programs).

39. *See*, *e.g.*, *supra* note 36, and *infra* note 40.

40. *See* HIPAA Regulations, *supra* note 6, 45 CFR pt. 164, subpts. A & C. 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."

41. 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." HIPAA Regulations, *supra* note 6, 45 CFR § 164.304.

42. *See* HIPAA Regulations, *supra* note 6, 45 CFR § 164.524.

43. *Id.* at § 164.526.

44. *Id.* at § 164.528.

45. *See id.* at § 164.508.

46. *Id.* at § 164.522.

47. *See* HITECH Omnibus Final Rule,, *supra* note 13, at 5628 - 30; *see also* HIPAA Regulations, *supra* note 6, 45 CFR § 164.522(a)(1)(iv).

48. HIPAA Regulations, *supra* note 6, 45 CFR § 164.528.

49. *Id.*

50. *Id.*

51. HITECH, *supra* note 10, § 13405(c)(1). 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."

and, consequently, better care for patients across the continuum of services.

However, as this article and our experience have shown, numerous important legal and regulatory implications arise in relation to the use of EHRs, the storage of PHI, and the "digitization" of health and medical information. Health care providers, and now cloud services 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.