KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

FAQ: HIPAA AND "CLOUD COMPUTING" (v1.0)

7 August 2013

"Cloud computing" – outsourcing core infrastructural computing functions to dedicated providers – holds great promise for health care. It can result in more flexible, powerful, and reliable health information services for providers large and small. There are a number of basic questions health care providers might ask when considering cloud computing: What is it? Why would a health care provider use it? What are the risks? Are cloud service providers business associates? In this Frequently Asked Questions (FAQ) document, the Health Privacy Project at the Center for Democracy & Technology answers these questions and more.

Note: The following is expert analysis and interpretation from CDT's Health Privacy Project and should not substitute for specific legal advice.

1. What is "cloud computing"?

Cloud computing is essentially "outsourcing" of organizational computing functions.

The National Institute of Standards and Technology (NIST) provides a technical definition of cloud computing:

> *Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*[1]

The basic idea behind cloud computing is to permit organizations such as health care providers to focus more on delivery of their core services without having to worry about constraints of their underlying network, computing infrastructure, operating systems, and software. There are generally three models for cloud computing services that organizations can use, depending on their needs:

Software as a service (SaaS): In this model, the cloud service provider (CSP) provides access to certain software functions, such as word processing, calendaring, and email. Software upgrades, updates, and maintenance are taken care of by the CSP. In most cases, health care providers will be operating under this model where specific software functions – e.g., a "cloud" based electronic health record service – are delivered by the CSP.

---

[1] "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Special Publication 800-145 (2011), *available at:* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Platform as a service (PaaS): Here the CSP provides customers with remotely accessible computing power, with which customers can install and run their own applications. Network access, system maintenance and updates, and configuration and provision of new computing power are all handled by the CSP, and customers do not have to worry about ongoing maintenance such as buying new hardware, migrating old data, and upgrading the operating system – they need only purchase access to additional compute power per their subscription with the CSP as needed. For example, a customer might purchase 10 "virtual servers" running a standard platform — such as the well-known "LAMP platform" consisting of the Linux operating system, Apache web server software, and MySQL database software — upon which the customer can then install custom or third party applications.

Infrastructure as a service (IaaS): In this model, the CSP focuses on providing hardware, networking and associated maintenance only. All aspects of the hardware configuration, operating systems, software installation, and maintenance are the responsibility of the customer.

Distinctions are sometimes drawn between "public" and "private" cloud services. This FAQ focuses on "public" cloud computing services — those in which health care entities use a third-party CSP for some or all of their cloud computing needs.

2. Can health care providers choose to store protected health information (PHI) in the "cloud," and why might they want to?

Yes, providers can store PHI in the cloud under HIPAA. Cloud computing can offer increased computing speed, capacity, flexibility, and security at significantly lower cost. Because CSPs focus entirely on ensuring reliable, high-availability access to information technology resources, health care organizations (like others) may find that it is substantially cheaper to obtain these resources from CSPs rather than trying to provide them on their own from within their organization. For example, while health care providers, particularly those with limited IT staff and budget, may find it difficult to make decisions about upgrades to software and hardware, CSPs will have routine processes in place for making and implementing those decisions. Cloud computing is very flexible and can scale to a health care provider's needs; large, unexpected changes in the needs of an organization are easy to accommodate in a cloud computing model. Cloud computing does not involve large upfront capital investments typical of more traditional computing infrastructure, and cloud computing makes it easier to cope with sudden shifts in resource needs. For example, if a hospital experiences an unexpected spike or dip in demand, it can simply adjust the amount of cloud computing resources it obtains from its CSP, instead of having to scramble to procure additional software and hardware or, alternatively, be left with superfluous technology it can't use.

CSPs can often provide a level of data security that health care providers could not achieve on their own. In particular, small health care providers that choose a good CSP may be able to attain a level of protection that it could not purchase or maintain on their own. However, as discussed below, a health care provider cannot *assume* that a CSP will adequately protect PHI under the HIPAA Security Rule. Rather, the health care provider must have reasonable assurances that the CSP is protecting information with at least the same diligence that the health care provider would be obligated to exercise with its own resources.

3. Is a cloud service provider (CSP) a business associate under the HIPAA Privacy Rule?

This question has been the subject of much debate recently. Based on our interpretation of the law, in most cases a CSP would be a business associate under HIPAA's Privacy Rule. Under the most recent version of the Privacy Rule, an entity that "creates, receives, *maintains*, or transmits protected health information (PHI)" in fulfilling certain functions or activities for a HIPAA-covered entity is considered to be a "business associate" (emphasis added).[2] Covered entities are required to execute agreements with their business associates – called business associate agreements (BAAs) – that set forth the permitted uses and disclosures of PHI by the business associate. Business associates that hire subcontractors to perform some of the services or functions requested by the Covered Entity must also execute business associate agreements with those subcontractors.

Most CSP arrangements with health care providers will involve the *maintenance* of PHI on the health care provider's behalf. In cases where the CSP is merely "transmitting" PHI for a covered entity, whether the CSP is or is not a business associate will depend on whether it requires access on a routine basis to such PHI. The HHS Office for Civil Rights (OCR), which enforces HIPAA, recently clarified that entities transmitting PHI are business associates under the final terms of the HITECH omnibus final rule only if they require access on a "routine basis" to such data.[3] If a contractor is a "mere conduit" for transmission of PHI – e.g., like the "conduit" role the postal service plays when health care providers send paper records in the mail – then it would not be considered a business associate. An Internet service provider (ISP) is an example of a digital "mere conduit." CSPs, on the other hand, typically perform functions that go farther than mere transmission services, such as storing, analyzing, reformatting or billing functions involving PHI.[4]

Some types of CSPs, even though they are maintaining PHI, may not have "routine access" to PHI. This has caused some confusion about the new business associate provisions, particularly since "routine access" is the test for determining whether or not an entity is more than a "mere conduit." For example, where the health care provider – not the CSP – encrypts PHI and holds the encryption keys, the CSP does not have the ability to access PHI.

However, in the most recent version of the Privacy Rule, OCR applied the test of "routine access" only to considerations of whether *transmission services* trigger the business associate definition. The definition of a business associate now expressly includes entities that "maintain" PHI on behalf of a covered entity, and "access" is not mentioned as relevant under that prong of the definition. According to OCR, maintenance includes persistent storage of PHI, beyond the type of temporary storage that might be necessary to ensure that a transmission of PHI

---

[2] 45 CFR 160.103, definition of "business associate" (at (3)(iii)).

[3] 45 CFR 160.103, definition of "business associate" (at (3)(i)) includes any entity "that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information."

[4] *See:* "HIPAA Final Rule Confirms That ISPs Transmitting PHI Are Not Business Associates," Center for Democracy & Technology (February 6, 2013), *available at:* https://www.cdt.org/blogs/joseph-lorenzo-hall/0602hipaa-final-rule-confirms-isps-transmitting-phi-are-not-business-assoc.

successfully reaches its designated endpoint.[5] PHI that is remotely stored in an encrypted format is still considered to be PHI, and thus subject to the Privacy Rule. Only when data has been de-identified per HIPAA Privacy Rule standards does it lose its status as PHI.

The obligations of a business associate depend on the extent of services and functions it is performing with PHI on behalf of a covered entity. A CSP that has no capability to access PHI, that provides storage functionality only, and that adheres to HHS standards with respect to encryption[6] should have little liability risk as a business associate (except to ensure that it properly manages encryption). Such an encrypted CSP should be able to enter into relatively simple BAAs compared to CSPs that maintain unencrypted PHI. For example:

- Provided that a covered entity and its associated encrypted CSP follow HHS guidance on encryption, a breach of encrypted PHI does not constitute a breach of unsecured PHI in terms of HHS' breach notification rule.[7]

- The elements required of a business associate agreement (BAA) – from 45 CFR 164.504(e)(2) – will be much more straightforward for an encrypted CSP that cannot access PHI. For example, if the covered entity controls the decryption keys and the CSP has no ability to access the plaintext of the data, it would not be reasonable to expect the CSP to comply with the provisions in 45 CFR 164.504(e)(2)(ii)(E)–(G) that require a BA to "make available" PHI for certain purposes.

4. Does cloud computing remove the need for health care providers to worry about the data they store with a CSP?

No. Cloud computing outsources *technical* infrastructure to another entity that essentially focuses all its time on maintaining software, platforms, or infrastructure. But a covered entity such as a health care provider still remains responsible for protecting PHI in accordance with the HIPAA Privacy and Security Rules, even in circumstances where the entity has outsourced the performance of core PHI functions. As noted above, in most cases, CSPs will be "business

---

[5] OCR wrote case-specific guidance in a 2003 letter to a secure *physical* document storage company, Tindall Record Storage. OCR stated for the *non-electronic* secure document storage case, "We confirm that a business associate agreement is not required between a covered entity and a document storage company performing functions on behalf of the covered entity, where any protected health information released to the storage company is transferred and maintained in closed and sealed containers, and the document storage company does not otherwise access the protected health information." (*See:* Letter from Richard M. Campanelli, Director for the Office of Civil Rights, Department of Health and Human Services, (May 12, 2003), appendix to: Tindall Record Storage, "Re: Comments regarding proposed rule RIN 0991-AB57" (September 1, 2010), *available at:* https://www.regulations.gov/#!documentDetail;D=HHS-OCR-2010-0016-0071.) However, OCR subsequently declined to issue general guidance for physical secure document storage (*Id.* at 2). The preamble to the omnibus HITECH final rule indicates that HHS was aware of this issue and declined to extend the "conduit exception" to persistent storage (of any form): "document storage companies maintaining protected health information on behalf of covered entities are considered business associates, regardless of whether they actually view the information they hold." (78 Fed. Reg. 5572).

[6] *See:* "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals," Department of Health and Human Services (September 14, 2009), *available at:* http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

[7] 45 CFR 164.400 *et seq.*

associates" and there will need to be a business associate agreement between the covered entity and the CSP.

Business associates also are directly accountable to regulators for complying with the HIPAA Security Rule, with selected provisions of the HIPAA Privacy Rule, and with their business associate agreements. In addition, business associates are obligated to inform covered entities of any breaches of PHI. However, this accountability does not release covered entities of their obligations under HIPAA. If a covered entity does not receive reasonable assurances from its business associates, it can be held accountable for noncompliance by the business associate in some circumstances. At the same time, regulators can hold business associates directly accountable for noncompliance. Depending on the circumstances surrounding the noncompliance, regulators would likely examine the specific facts and determine liability accordingly. (See the discussion below in FAQ 8 for an example of a covered entity that did not fulfill its obligations in this respect and was subject to HHS enforcement.)

5. Can the government access PHI stored with a CSP for law enforcement and national security purposes?

HIPAA generally allows government agencies to demand disclosure of health records for national security and law enforcement purposes.[8] A government request may be made directly to a CSP. While disclosure demands for national security purposes are likely to be rare, under Section 215 of the PATRIOT Act the government can require a CSP to produce PHI under a secret, gagged order, such that the covered entity may never learn that such production of PHI occurred. Of course, if the CSP is an encrypted CSP, and it does not have the decryption keys, it will only be able to turn over encrypted data.

6. How important is it for health care providers to choose CSPs that claim they are "HIPAA compliant"?

"HIPAA compliance" is not a certification or compliance regime formally recognized by the Department of Health and Human Services. Accordingly, health care providers should be wary of overreliance on claims from CSPs that they are "certified" or otherwise "HIPAA compliant." The CSP should be willing to enter into a business associate agreement and acknowledge its obligations to comply with HIPAA and other applicable regulations. Health care providers will need to carefully choose a good CSP that has a track record of working securely with PHI and is familiar with obligations of business associates under HIPAA. Claims of "HIPAA compliance" should be appropriately vetted. That being said, there are standard purpose-specific types of certifications that a health care provider should consider when selecting a CSP, including: PCI-DSS (credit card transaction standards), SSAE 16 (financial reporting standards), ISO 27001 (information security standards), and FIPS 140 (cryptographic module standards).

[8] Christopher Rasmussen, "Law Enforcement & National Security Access to Medical Records," Center for Democracy & Technology, (2013), *available at:* https://www.cdt.org/policy/law-enforcement-national-security-access-medical-records

7. Can health care providers use general purpose, publicly available Internet services such as document, email, and calendar services to store PHI and still be in compliance with HIPAA?

Covered entities or individual employees of covered entities may find it convenient to use general purpose document, email, or calendar services that are publicly available on the Internet to store PHI, but the use of such services may be risky. Health care providers will need to choose CSPs that enable compliance with HIPAA, which may not be the case for cloud services offered generally to the public over the Internet. The most immediate problem is that health care providers are required to execute BAAs with any entity that "creates, receives, maintains, or transmits PHI" on their behalf, and a general purpose, publicly available service may not have customizable terms of service that comply with the requirements for a BAA. In addition, aspects of these tools could result in HIPAA violations or data breaches. For example, if a covered entity misconfigured a service such that it accidentally displayed PHI publicly, that would almost certainly be a HIPAA violation on the part of the covered entity.[9] There has been at least one enforcement case brought by HHS that found violations in exactly this case (see item 8).

8. Has HHS brought HIPAA enforcement actions based on the use of cloud services?

Yes. The Department of Health and Human Service's Office for Civil Rights settled with a firm, Phoenix Cardiac Surgery, in 2012 for extensive violations of the HIPAA Privacy and Security Rules, including the inappropriate use of cloud services. Specifically, HHS found that Phoenix Cardiac Surgery "was posting clinical and surgical appointments for its patients on an Internet-based calendar that was publicly accessible" and that it had failed to enter into a business associate agreement with the CSP in question, despite the service storing and being able to access PHI.[10] The settlement included monetary penalties of $100,000 and a multi-year corrective action plan to bring Phoenix Cardiac Surgery into full compliance.

For further information, contact:

- Health Privacy Project Director, Deven McGraw (202-407-8833, deven@cdt.org)
- Senior Staff Technologist, Joseph Lorenzo Hall (202-407-8825, joe@cdt.org).

[9] When a health care provider decides to use a mainstream cloud service provider to store PHI, we do not think that puts the CSP itself in violation of HIPAA unless the CSP is directly marketing its services to the HIPAA covered entity community and presuming it can avoid business associate liability by not signing BAAs.

[10] Press Release, "HHS settles case with Phoenix Cardiac Surgery for lack of HIPAA safeguards," Department of Health and Human Services (April 17, 2012), *available at:* http://www.hhs.gov/news/press/2012pres/04/20120417a.html.