Guidance on HIPAA & Cloud Computing

From the US Department of Health & Human Services

For your convenience, below are relevant excerpts from the 8-page HHS Guidance, which can be read in its entirety here: http://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

Introduction

With the widespread adoption of cloud computing solutions, HIPAA covered entities and business associates are questioning how they can take advantage of cloud computing while complying with regulations protecting the privacy and security of electronic protected health information (ePHI). This guidance assists such entities, including cloud services providers (CSPs), in understanding their HIPAA obligations.

Common cloud services are on-demand internet access to computing services such as networks, servers, storage, and applications. CSPs generally offer online access to shared computing resources ranging from simple data storage to complete software solutions (e.g., an EMR system), platforms to simplify the ability of application developers to create new products, and entire computing infrastructure for software programmers to deploy and test programs.

When you, as a covered entity, engage a cloud services provider to create, receive, maintain, or transmit ePHI (such as to process and/or store ePHI) on your behalf, that CSP is a business associate and as such must comply with the applicable provisions of the HIPAA Rules.

Further, when one of your business associates subcontracts with a CSP to create, receive, maintain, or transmit ePHI on your behalf, the subcontractor is also a business associate. As a result, you or your business associate must enter into a HIPAA-compliant business associate agreement (BAA) with the CSP, who is then contractually liable for meeting the terms of the BAA and directly liable for compliance with the applicable HIPAA requirements.

List of Questions Answered

1. May a covered entity or business associate use a cloud service to store or process ePHI?
2. If a CSP stores only encrypted ePHI and does not have a decryption key, is it a HIPAA business associate?
3. Can a CSP be considered to be a "conduit" like the postal service, and, therefore, not a business associate that must comply with the HIPAA Rules?
4. Which CSPs offer HIPAA-compliant cloud services?
5. What if a covered entity (or business associate) uses a CSP to maintain ePHI without first executing a business associate agreement with that CSP?
6. If a CSP experiences a security incident involving a covered entity's or business associate's ePHI, must it report the incident to the covered entity or business associate?
7. Do the HIPAA Rules allow health care providers to use mobile devices to access ePHI in a cloud?
8. Do the HIPAA Rules require a CSP to maintain ePHI for some period of time beyond when it has finished providing services to a covered entity or business associate?

9. Do the HIPAA Rules allow a covered entity or business associate to use a CSP that stores ePHI on servers outside of the United States?
10. Do the HIPAA Rules require CSPs that are business associates to provide documentation, or allow auditing, of their security practices by their customers who are covered entities or business associates?
11. If a CSP receives and maintains only information that has been de-identified in accordance with the HIPAA Privacy Rule, is it is a business associate?

Q & A

Below are the HHS answers, in abbreviated form designed for easier understanding. For detailed answers, please read the 8-page HHS Guidance.

1. May a covered entity or business associate use a cloud service to store or process ePHI?

Yes, provided the covered entity or business associate enters into a HIPAA-compliant business associate agreement (BAA) with the CSP and otherwise complies with HIPAA Rules.

2. If a CSP stores only encrypted ePHI and does not have a decryption key, is it a HIPAA business associate?

Yes, because the CSP receives and maintains (e.g., to process and/or store) electronic protected health information (ePHI) for a covered entity or another business associate.

3. Can a CSP be considered to be a "conduit" like the postal service, and, therefore, not a business associate that must comply with the HIPAA Rules?

Generally, no. CSPs that provide cloud services to a covered entity or business associate that involve creating, receiving, or maintaining (e.g., to process and/or store) ePHI meet the definition of a business associate, even if the CSP cannot view the ePHI because it is encrypted and the CSP does not have the decryption key.

4. Which CSPs offer HIPAA-compliant cloud services?

HHS OCR does not endorse, certify, or recommend specific technology or products.

5. What if a covered entity or business associate uses a CSP to maintain ePHI without first executing a business associate agreement with that CSP?

The covered entity or business associate is in violation of the HIPAA Rules. A CSP that creates, receives, maintains, or transmits PHI on behalf of a covered entity or another business associate must comply with all applicable provisions of the HIPAA Rules, regardless of whether it has executed a BAA with the entity using its services.

6. If a CSP experiences a security incident involving a covered entity's or business associate's ePHI, must it report the incident to the covered entity or business associate?

Yes. The Security Rule requires business associates to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the business associate; and document security incidents and their outcomes. A business associate agreement must require the business associate to report, to the covered entity or business associate whose ePHI it maintains, any security incidents of which it becomes aware.

A security incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. The Security Rule does not prescribe the level of detail, frequency, or format of reports of security incidents; these may be worked out between the parties to the business associate agreement (BAA). For incidents that rise to the level of a breach, the Breach Notification Rule specifies the content, timing, and other requirements for reporting.

7. Does HIPAA allow health care providers to use mobile devices to access ePHI in a cloud?

Yes. Health care providers, other covered entities, and business associates may use mobile devices to access ePHI in a cloud. Appropriate physical, administrative, and technical safeguards must be in place to protect the confidentiality, integrity, and availability of the ePHI on the mobile device and in the cloud. Appropriate BAAs must be in place with any third party service providers for the device and/or the cloud that will have access to the ePHI.

8. Does HIPAA require a CSP to maintain ePHI for some period of time after it has finished providing services to a covered entity or business associate?

No. The Privacy Rule provides that a business associate agreement (BAA) must require a business associate to return or destroy all PHI at the termination of the BAA where feasible. If such return or destruction is not feasible, the BAA must extend the privacy and security protections of the BAA to the ePHI and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

9. Do the HIPAA Rules allow a covered entity or business associate to use a CSP that stores ePHI on servers outside of the United States?

Yes, provided the covered entity or business associate enters into a business associate agreement (BAA) with the CSP and otherwise complies with the applicable HIPAA requirements. However, the HHS Office for Civil Rights notes that the risks to such ePHI may vary greatly depending on the CSP's geographic location. Covered entities, and business associates including the CSP, should take these risks into account when conducting the risk analysis and risk management required by the Security Rule.

10. Are CSPs who are business associates required to provide documentation, or allow auditing, of their security practices by their customers who are covered entities or business associates?

No. HIPAA requires covered entity and business associates to obtain satisfactory assurances in the business associate agreement (BAA) that the CSP will appropriately safeguard the protected health information (PHI) that it creates, receives, maintains or transmits for the covered entity or business associate in accordance with HIPAA Rules. The CSP is also directly liable for failing to safeguard electronic PHI and for impermissible uses or disclosures of the PHI.

11. If a CSP receives and maintains only information that has been de-identified in accordance with the HIPAA Privacy Rule, is it a business associate?

No. De-identified information is not considered protected health information, and therefore a CSP is not a business associate if it receives and maintains only information de-identified following the processes required by the Privacy Rule.

The complete, 8-page HHS Guidance can be read in its entirety here: http://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html