GUIDANCE ON HIPAA & CLOUD COMPUTING

http://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

January 26, 2017

Health Care Cloud Coalition

Deven McGraw, Deputy Director, Health Information Privacy

Purpose

- To assist HIPAA covered entities (CEs) and business associates (BAs), in understanding their HIPAA obligations to protect the privacy and security of electronic protected health information (ePHI) when they take advantage of cloud technologies

Covered Entities

- Health Plan
- Health Care Clearinghouse
- Health Care Providers that conduct certain payment related transactions electronically

Definition of Business Associate

… a person who: (i) On behalf of such covered entity… **creates, receives, maintains, or transmits protected health information** for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration… or (ii) **Provides … services** to or for such covered entity, … …involves the disclosure of protected health information from such covered entity…to the person.

…includes: …other person that provides **data transmission services…that requires access on a routine basis** to such protected health information. (ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.. (iii) **A subcontractor** that creates, receives, maintains, or transmits protected health information on behalf of the business associate….

45 CFR 160.103 Definitions

Cloud Service Provider (CSP)

- Offers online access to shared computing resources
- Functions and scale can vary in response to user demands
- Services may include on-demand internet access to
  - Data storage
  - Applications, software solutions (e.g., electronic health record system, email, databases)
  - Networks, servers

CSPs are Business Associates…

- When a covered entity engages the services of a CSP *to create, receive, maintain, or transmit* ePHI on its behalf, the CSP is a business associate under HIPAA
- When a business associate of a covered entity subcontracts with a CSP *to create, receive, maintain, or transmit* ePHI for purposes of assisting the business associate in performing functions or services for the covered entity, the CSP subcontractor is a business associate of the original business associate

If CSP is a BA

- CE & CSP, or BA & CSP, must establish HIPAA-compliant business associate agreements (BAA)
- CSP is liable to
  - CE, or other BA, for meeting the terms of the agreement
  - Directly liable to HHS for compliance with the applicable requirements of the HIPAA Rules

Central Guidance Points

- HIPAA covered entities and business associates can use the services of CSPs consistent with their HIPAA responsibilities
- A CSP can be a BA when it processes or stores only encrypted ePHI and lacks an encryption key for the data
  - Lacking an encryption key does ***not*** exempt a CSP from business associate status and obligations under the HIPAA Rules

- May a covered entity or business associate use a cloud service to store or process ePHI? ***YES***
  - CE and the CSP must enter into a business associate agreement (contract containing particular terms)
    - Establishes permitted and required uses and disclosures of ePHI
    - Requires BA to appropriately safeguard the ePHI
  - CE may want to understand cloud environment of the CSP for its own risk management, and proper drafting of its BAA and any service level agreement
    - E.g., cloud configuration may impact RA/RM
    - SLA must be consistent with Rules

Questions 2

- If a CSP stores only encrypted ePHI and does not have a decryption key, is it a business associate?
- Yes, because it receives, transmits and maintains ePHI-- *even if it cannot view the ePHI*. We refer to these as *no-view* services in guidance
  - Lacking a decryption key does not alone assure the confidentiality, integrity & availability of ePHI
  - Guidance walks through considerations for addressing particular requirements of the Rules, e.g., implementing appropriate access controls
  - Entities should document how each party will address requirements

- Where contractual agreements between CSP and CE/BA customer provide that customer will control and implement certain security features of the cloud service consistent with the SR, and the customer fails to do so--
  - A BA is not responsible for the compliance failures that are attributable solely to the actions or inactions of the CE, as determined by the facts and circumstances of the particular case

Questions 4

- 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?
  - Unlikely, as the conduit exception is limited to transmission-only services and temporary storage of PHI incident to those transmissions

- Which CSPs offer HIPAA compliant cloud services?
  - OCR does not endorse certify or recommend specific technology or products

- What if a covered entity (or BA) uses a CSP for ePHI without first executing a BA agreement with CSP ?
  - The CE is in violation of the HIPAA Rules
  - CSP that is a BA must comply with Rules regardless of whether it has executed a BAA with the CE using its services
  - When CSP discovers that a CE or BA customer is using its cloud for ePHI, it must either
    - come into compliance , & enter into a BAA or
    - securely return the ePHI to the customer or, if agreed to by the customer, securely destroy the ePHI

- 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. SR requires BA to identify, respond to, mitigate and document security incidents, & must report to CE or BA re their ePHI
  - SR flexible—may use the BAA to set type, detail, frequency of reports, e.g., report # of pings monthly
  - BNR does specify content, timing etc. re incidents that rise to the level of a breach of unsecured PHI

- Do the HIPAA Rules allow health care providers to use mobile devices to access ePHI in a cloud?
  - Yes
  - Implement appropriate safeguards
  - Enter into BAAs with any third party service providers for the device and/or cloud that will have access to the ePHI
- OCR, FTC and ONC guidance available on this topic
  - http://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device

- 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?
  - No. A BAA must require a business associate to return or destroy all PHI at the termination of the BAA where feasible
  - If not feasible, the BAA must extend 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 (e.g., other law re document retention)
  - *Note, this is further explored in Data Availability FAQ*

- 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. Same requirements apply
  - However, a CE would need to consider the location of the BA in its risk analysis and risk management, as outsourced storage overseas may present special considerations/increased vulnerabilities

- Must CSPs that are business associates provide documentation or allow auditing of their security practices by their customers who are covered entities or business associates?
  - The Rules require assurances in the form of the BAA. CEs may require additional assurances from BAs as part of their risk management
- 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?
  - No. Such de-identified information is not PHI

Guidance Refers Reader To

- NIST publications, e.g., defining cloud computing
  - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
- Existing OCR FAQs & guidance documents, e.g., sample contract provisions
  - http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
- ONC resources, e.g., recommendations for EHRs
  - http://www.healthit.gov/providers-professionals/ehr-privacy-security