U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

June 2017

File Sharing and Cloud Computing: What to Consider?

The implementation of file sharing and collaboration tools, including tools that leverage cloud technology, brings with it additional security concerns that HIPAA covered entities and business associates must take into account in their risk analyses, risk management policies, and business associate agreements (BAAs). Cloud computing and file sharing services can introduce additional risks to the privacy and security of electronic protected health information (ePHI) that organizations must identify as part of their risk analysis process and mitigate as part of their risk management process.

For example, a recent survey regarding file sharing and collaboration tools used by organizations from a variety of industries including the healthcare industry, found that just under half of the surveyed organizations stated that they had at least one confirmed file sharing data breach in the last two years.[1] Respondents of this survey listed as their top security concerns: temporary workers, contractors, or third parties accessing data they should not see; employees accidentally exposing data; and broken security management processes.[2] Only twenty-eight percent of respondents listed external hackers as one of their top three concerns.[3]

Additionally, misconfigurations of file sharing and collaboration tools, as well as cloud computing services, are common issues that can result in the disclosure of sensitive data, including ePHI. Too often, access, authentication, encryption and other security controls are either disabled or left with default settings, which can lead to unauthorized access to or disclosure of that data.

Many of these misconfigurations and errors should be detected and corrected as part of an organization's risk analysis and risk management processes or as a result of its evaluation process in response to environmental or operational changes within the organization. As part of that process, vulnerability scans may help to identify technical vulnerabilities such as missing patches, obsolete software, and misconfigurations of many common file sharing and collaboration tools.

These security concerns are not unique to any particular file sharing or cloud computing technology. Thus, when using these technologies, covered entities and business associates

---

[1] Ponemon/Metalogix, *Handle with Care: Protecting Sensitive Data in Microsoft SharePoint, Collaboration Tools and File Share Applications*, https://pages.metalogix.com/ebook-sensitive-data-sharepoint.html, 1.
[2] *Id*. at 4.
[3] *Id*.

must conduct an accurate and thorough risk analysis, adopt risk management policies to ensure risks are reduced to a reasonable and appropriate level, and enter into comprehensive BAAs (and SLAs where appropriate) to ensure the protection of ePHI and compliance with the HIPAA Rules before implementing any file sharing or cloud computing service that will be creating, receiving, maintaining, or transmitting ePHI.

OCR Cloud Computing Guidance

The U.S. Department of Health and Human Services, Office for Civil Rights (OCR) issued guidance in October 2016 to assist covered entities and business associates that decide to utilize cloud computing services how they can leverage cloud technologies while complying with the HIPAA Privacy, Security and Breach Notification Rules (the HIPAA Rules) protecting the privacy and security of ePHI. This guidance addresses key issues, including:

- A cloud service provider (CSP) is a business associate when a covered entity or business associate engages the services of the CSP to create, receive, maintain, or transmit ePHI (such as to process and/or store ePHI) on its behalf.
- The CSP lacking an encryption key to the ePHI does not exempt the CSP from business associate status and its obligations under the HIPAA Rules.
- A HIPAA-compliant BAA is required between the covered entity (or business associate) and the CSP.
- OCR does not endorse, certify, or recommend specific technology or products.
- In addition to a BAA, a Service Level Agreement (SLA) is commonly used to address more specific business expectations between the CSP and its customer (the covered entity or business associate). SLAs, consistent with the BAA, may address HIPAA concerns such as:
    - System availability and reliability;
    - Back-up and data recovery;
    - Manner in which data will be returned to the customer after service termination;
    - Security responsibility; and
    - Use, retention and disclosure limitations.

These are only some highlights from the guidance, which contains eleven key questions and detailed answers. It is important to note that OCR also does not endorse or otherwise recognize private organizations' "certifications" regarding HIPAA compliance, and covered entities and business associates should ensure their own compliance with the HIPAA Rules.

Read the full guidance: https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html.

For more information on HIPAA and Cloud Computing, see:

1. OCR's Guidance on HIPAA & Cloud Computing, https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html#_ftnref1
2. SP 800-145, The NIST Definition of Cloud Computing, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

3. NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing, http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909494
4. NIST SP 800-146, Cloud Computing Synopsis and Recommendations, http://www.nist.gov/manuscript-publication-search.cfm?pub_id=911075