MARSH & McLENNAN AGENCY

SPECIAL ALERT

Volume Thirteen, Issue Five October 2017

FILE SHARING GUIDANCE

The Office of Civil Rights (OCR) recently released a bulletin on file sharing and collaboration tools. Collaboration tools can use cloud technology. These tools, bring additional security concerns that may affect compliance with the Health Insurance Portability and Accountability Act's (HIPAA's) Security Rules. Because cloud computing and file sharing services may result in security risks to Electronic Protected Health Information (EPHI), covered entities need to review their security risks before they use these tools. Covered entities need to think about how they will use these types of services to share EPHI. They may need
business associate agreements with the cloud or file-sharing vendor.

A recent healthcare industry survey by Ponemon/Metalogix found just under half of survey respondents had at least one confirmed file sharing data breach in the last two years. The survey respondents top security concerns are as follows:

- temporary workers
- contractors
- third-party vendors accessing data without authorization
- employees accidently exposing data
- broken security management processes

Only 28 percent of respondents listed external hackers as one of their top three security concerns.

Often covered entities do not understand the level of security protecting their data when they use file sharing or cloud computing services. Access, authentication, encryption or other security controls are frequently disabled or left in the default setting. Covered entities could be compromising the security of sensitive data when they merely assume security controls are in place.

Covered entities should review their risk management process to check into some of these issues. They should conduct a risk management review when they choose a vendor for file sharing or a cloud computing service. These types of security scans will also identify technical

Continued on Page 2

We welcome your comments and suggestions regarding this issue of our Special Alert. For more information, please contact your Account Manager or visit our website at www.mma-mi.com.

vulnerabilities such as missing patches, obsolete software and any misconfigurations of the file sharing tools. Covered entities may want to consider limiting the file sharing or cloud computing options to vendors that have been vetted for security. This is critical if sensitive information is shared on these services.

The bulletin provides more details for covered entities that choose to use cloud technologies to comply with HIPAA security and breach notification rules. Key points include:

- A cloud service provider (CSP) is considered a business associate when the covered entity engages the CSP to create, receive, maintain or transmit EPHI.
- Even if a CSP lacks an encryption key to the EPHI, it is not exempt from business associate status and its HIPAA obligations.
- A HIPAA compliant business associate agreement is required between the CSP and the covered entity.
- In addition to a business associate agreement, a covered entity may want to secure a Service Level Agreement (SLA) with a CSP. SLAs may cover some HIPAA Security concerns such as:
  - System availability and reliability
  - Back-up and data recovery
  - How data will be returned to the customer after service termination
  - Use, retention and disclosure limitations

The OCR also provided these links to other resources on cloud computing:

- Full guidance: https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
- National Institute of Standards and Technology guidance:
  - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
  - https://www.nist.gov/publications/guidelines-security-and-privacy-public-cloud-computing?pub_id=909494
  - https://www.nist.gov/publications/cloud-computing-synopsis-and-recommendations?pub_id=911075

If you use cloud computing in your organization, these documents will help you apply security protocols to protect your data.

CONCLUDING THOUGHTS

The DOL and OCR continue to publish bulletins to inform employers how HIPAA Security Rules apply to covered entities as they expand the number of service providers they use in the electronic data realm.

It is critical for an organization to review HIPAA Security procedures whenever new technology that could be used to house or share EPHI is introduced. In addition, organizations should review security protocols whenever they upgrade technologies. The OCR is very focused on efforts organizations are making to secure EPHI. MMA

Marsh & McLennan Agency LLC

Health & Benefits
3331 West Big Beaver Road, Suite 200
Troy, MI 48084
Telephone: 248-822-8000 Fax: 248-822-4131
www.mma-mi.com

Property & Casualty
15415 Middlebelt Road
Livonia, MI 48154
Telephone: 734-525-0927 Fax: 734-525-0612
www.mma-mi.com