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

# May 2017

# *Cybersecurity Incidents will happen…*
# *Remember to Plan, Respond, and Report!*

## *The Incident Headlines*

**Leading Cause of Healthcare Data Breaches in April was Hacking**

- *HIPAA Journal.com, May 23, 2017*

**Top 10 sub-sectors breached by number of incidents Business Services was the most affected sub-sector, followed by Health Services in 2016**

- *Internet Security Threat Report, by Symantec, April 2017*

**Healthcare Data Security Incidents Second Highest in 2016**

- *Health IT Security.com*

**Ransomware Attack: Healthcare Vulnerable to Cyber Attacks**

- *Fortune.com, May 15, 2017*

Heath information technology systems are expected to provide security controls that will ensure the confidentiality, integrity, and availability of protected health information (PHI). However, having robust and fairly resilient systems doesn't eliminate the possibility that a cyber-incident will occur, as shown by recent news headlines.

Incidents do happen and when they do, effective response planning can be a major factor of how significant an organization suffers operational or reputational harm or legal liability. Being able to respond to incidents in a systematic way ensures that appropriate response steps are taken each time to help minimize the impact of breaches.

## *Refresher – What's a Security Incident? When is it a Breach?*

*The HIPAA Security Rule defines a security incident as an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. (See the definition of security incident at 45 CFR 164.304.) The HIPAA Breach Notification Rule defines a breach as, generally, an impermissible acquisition,* *access, use, or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the protected health information. (See the definition of breach at 45 CFR 164.402.)*

## *Handling an Incident – An Incident Occurs; How's your Capability to Respond?*

An incident response policy and different types of contingency plans assist Covered Entities and Business Associates in having a proper, concentrated, and coordinated approach to responding to incidents. These policies, procedures, and plans should provide a roadmap for implementing the entity's incident response capabilities. They should also meet the Covered Entities' and Business Associates' distinctive requirements that relates to their mission, sizes, structures, and functions, and identify the necessary resources and management support. They should be approved by management, reviewed and tested regularly, and should include the entity's processes for:

- preparing for incidents, including assessing the criticality of applications and data;
- detecting and analyzing incidents;
- implementing disaster recovery and emergency operations, as applicable;
- containing, eradicating and recovering from incidents, including implementing data backup; and
- conducting post-incident activities and reviews.

## *Information Sharing – Coordination and Communicate*

The nature of existing threats and attacks makes it more important than ever for organizations to work together during incident response. The Federal Government has recognized the importance of information-sharing in the cybersecurity context, reflective in legislation such as the Cybersecurity Information Security Act (CISA) and Executive Order 13691.

Information Sharing is where different organizations share threat, attack, and vulnerability information with each other so that each organization's knowledge benefits the other. Covered Entities and Business Associates should consider the best ways to share cyber threat indicators during incidents, while not sharing PHI, and with whom to share those indicators.

## *Breach Reporting – Prompt Notice to Help Mitigate Potential Harm*

Once it has been established a breach has occurred, breach reporting is an important part of the incident management process. Timely reporting helps to identify and rectify problems with individual organizations, identify and assess emerging risks, and protect individuals from identity theft or other fraud.

The HIPAA Breach Notification Rule requires covered entities to notify affected individuals, OCR, and in some cases, the media of a breach of unsecured protected health information (PHI).  Most notifications must be provided without unreasonable delay and no later than 60 days following the discovery of a breach. Notifications of smaller breaches affecting fewer than 500 individuals may be submitted to OCR annually. The Breach Notification Rule also requires business associates of covered entities to notify the covered entity of breaches at or by the business associate. Visit the HHS HIPAA Breach Notification Rule webpage for more information and guidance on the reporting requirements.

## Resources:

**Industrial Control Systems Cybersecurity Emergency Response Team (ICS-CERT):** ICS-CERT Releases WannaCry Fact Sheet

**Office for Civil Rights (OCR):** http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html - *(HIPAA Breach Notification Guidance)*

https://www.hhs.gov/hipaa/for-professionals/faq/2072/covered-entity-disclose-protected-health-information-purposes-cybersecurity-information-sharing/ - *(HIPAA Information-Sharing FAQ)*

**Congress.Gov:** *https://www.congress.gov/bill/114th-congress/senate-bill/754/text (Cybersecurity Information Security Act)*

**Department of Homeland Security (DHS):** https://www.dhs.gov/isao *(Information Sharing and Analysis Organizations)*