U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE FOR CIVIL RIGHTS

OCR Update

September 29, 2016

National Committee on Vital and Health Statistics

Rachel Seeger, Senior Advisor

HHS Office for Civil Rights (OCR)

Enforcement Update

Catholic Health Care Services – June 29, 2016

- CHCS agreed to settle potential violations of the HIPAA Security Rule after the theft of a mobile device compromised the protected health information (PHI) of hundreds of nursing home residents.
- CHCS provided management and information technology services as a business associate to six skilled nursing facilities.
- The total number of individuals affected by the combined breaches was 412.
- The settlement includes a monetary payment of $650,000 and a corrective action plan.

Oregon Health & Science University - July 18, 2016

- $2,700,000 settlement to resolve potential violations of the HIPAA Privacy and Security Rules, as well as a comprehensive three-year corrective action plan.
- OCR's investigation began after OHSU submitted multiple breach reports affecting thousands of individuals, including two reports involving unencrypted laptops and another large breach involving a stolen unencrypted thumb drive.
- The investigation uncovered evidence of widespread vulnerabilities within OHSU's HIPAA compliance program, including the storage of the electronic protected health information (ePHI) of over 3,000 individuals on a cloud-based server without a business associate agreement.
- OCR found significant risk of harm to 1,361 of these individuals due to the sensitive nature of their diagnoses.

University of Mississippi Medical Center - July 21, 2016

- OCR's investigation of UMMC was triggered by a breach of unsecured electronic protected health information ("ePHI") affecting approximately 10,000 individuals.
- During the investigation, OCR determined that UMMC was aware of risks and vulnerabilities to its systems as far back as April 2005, yet no significant risk management activity occurred until after the breach, due largely to organizational deficiencies and insufficient institutional oversight.
- UMMC paid a resolution amount of $2,750,000 and will adopt a corrective action plan to help assure future compliance with HIPAA Privacy, Security, and Breach Notification Rules.

Advocate Health Care – August 4, 2016

- This settlement of $5.55 million, the largest to-date against a single entity, is a result of the extent and duration of the alleged noncompliance (dating back to the inception of the Security Rule in some instances), and the large number of individuals whose information was affected by Advocate, one of the largest health systems in the country.
- Advocate submitted three breach notification reports pertaining to separate and distinct incidents affecting the ePHI of approximately 4 million individuals.
- Lack of an accurate and thorough risk assessment and risk management policies and procedures.
- Failure to obtain a written business associate contract
- Failure to reasonably safeguard an unencrypted laptop when left in an unlocked vehicle overnight.

Care New England Health System - September 23, 2016

- Notification from Woman & Infants Hospital of Rhode Island (WIH), a covered entity member of CNE, of the loss of unencrypted backup tapes containing the ultrasound studies of approximately 14,000 individuals, including patient name, data of birth, date of exam, physician names, and, in some instances Social Security Numbers.
- As WIH's business associate, CNE provides centralized corporate support including technical support and information security for WIH's information systems.
- WIH provided OCR with a business associate agreement with Care New England Health System effective March 15, 2005, that was not updated until August 28, 2015, as a result of OCR's investigation, and therefore, did not incorporate revisions required under the HIPAA Omnibus Final Rule.
- The settlement includes a monetary payment of $400,000 and a comprehensive corrective action plan.

OCR's Small Breach Initiative

Beginning in August, 2016, OCR has begun an initiative to more widely investigate the root causes of breaches affecting fewer than 500 individuals. Among the factors Regional Offices will consider include:

- The size of the breach;
- Theft of or improper disposal of unencrypted PHI;
- Breaches that involve unwanted intrusions to IT systems (for example, by hacking); The amount, nature and sensitivity of the PHI involved; or
- Instances where numerous breach reports from a particular covered entity or business associate raise similar issues.

Regions may also consider the lack of breach reports affecting fewer than 500 individuals when comparing a specific covered entity or business associate to like-situated covered entities and business associates.

Policy Update

Availability of PHI maintained by a Business Associate

- On September 28, OCR issued a new FAQ clarifying that a business associate of a HIPAA covered entity may not block or terminate access by the covered entity to the protected health information (PHI) maintained by the business associate for or on behalf of the covered entity.
- For example, a business associate blocking access by a covered entity to PHI (such as where an EHR developer activates a “kill switch” embedded in its software that renders the data inaccessible to its provider client) to resolve a payment dispute with the covered entity is an impermissible use of PHI.
- In the event of termination of the agreement by either party, a business associate must return PHI as provided for by the business associate agreement. If a business associate fails to do so, it has impermissibly used PHI.
- Second, a business associate is required by the HIPAA Security Rule to ensure the confidentiality, integrity, and availability of all ePHI that it creates, receives, maintains, or transmits on behalf of a covered entity.
- Maintaining the availability of the ePHI means ensuring the PHI is accessible and usable upon demand by the covered entity, whether the PHI is maintained in an EHR, cloud, data backup system, database, or other system.

HIPAA and Unique Device Identifiers July 27, 2016

- OCR has posted a new FAQ on HIPAA and Unique Device Identifiers (UDI), which clarifies that the device identifier (DI) portion of a UDI can be part of a limited or de-identified data set as defined under HIPAA.
- While the HIPAA Privacy Rule prohibits the inclusion of "device identifiers and serial numbers" in both limited data sets and data sets that are de-identified in accordance with the "de-identification safe harbor" provisions, the guidance explains that the DI portion of the UDI is not the type of "device identifier" to which these HIPAA Privacy Rule provisions refer.

Cybersecurity Newsletters

August: Insider Threats

- According to a survey recently conducted by Accenture and HfS Research, 69% of organization representatives surveyed had experienced an insider attempt or success at data theft or corruption.
- Further, it was reported by a Covered Entity that one of their employees had unauthorized access to 5,400 patient's ePHI for almost 4 years.
- Best practices include developing policies and procedures to mitigate the possibility of theft of ePHI, sabotage of systems or devices containing ePHI, and fraud involving ePHI; Conducting screening processes on potential employees; and knowing your assets

September: Cyber Threat Information Sharing

- Covered Entities and Business Associates can help each other prepare for possible threats or vulnerabilities to ePHI systems by sharing information
- NIST's ***Guide to Cyber Threat Information Sharing*** identifies benefits and challenges for organizations participating in information sharing activities
- OCR issued an FAQ on what type of information can be disclosed by Covered Entities and Business Associates in this context.

What's to Come

- Cloud guidance
- Guidance on text messaging
- Social media guidance
- PMI and research authorizations
- ANPRM to solicit views on ways in which an individual who is harmed by an offense punishable under HIPAA may receive a percentage of any CMP or monetary settlement collected

Audit

Guidance for 2016 HIPAA Desk Audits

- Covered entities received notification of their selection as the subjects of OCR desk audits of compliance with the HIPAA Security, Privacy and Breach Notification Rules.
- They were also invited to participate in a webinar held on Wednesday, July 13, where OCR staff walked through the processes they can expect for the audit and expectations for their participation.
- Desk audits require entities to submit documentation of their compliance with requirements of the notice of privacy practices, access, breach notification, risk analysis and risk management standards.
- Desk audits of business associates will take place this Fall.

2016 OCR/NIST Conference

- October 19-20, 2016
- Keynote on Day 2 by Walter Suarez, MD
- Sessions include:
  - Identity Management and Access Controls
  - Business Associate Liability
  - Best Defense Tactics Against Ransomware
  - Updates from FTC, Health Care Industry Cybersecurity Task Force, ONC and OCR

Questions?

http://www.hhs.gov/hipaa

Join us on Twitter @hhsocr