U.S. DEPARTMENT OF
HEALTH AND HUMAN SERVICES

OFFICE FOR
CIVIL RIGHTS

OCR Update

November 30, 2016
National Committee on Vital and Health Statistics
Rachel Seeger, Senior Advisor
HHS Office for Civil Rights (OCR)

Enforcement Update

Highlights

- OCR has issued its Reports to Congress for 2013 and 2014 on Compliance and Enforcement, and Breach Notification. We have also posted our 2015 annual numbers.
- The reports and data highlight that most of OCR's work centers on the investigation of breach reports and other reports of systemic noncompliance with HIPAA.
- Further, in 2015 and 2016, we've entered into a record number of settlement agreements.
- OCR continues to focus its enforcement efforts and its resources in this area on cases that identify industry-wide noncompliance, where corrective action under HIPAA may be the only remedy, and where corrective action benefits the greatest number of individuals.

We hope that our resolution agreements will provide a template for other health care entities to take the proactive steps necessary to ensure compliance with HIPAA requirements.

UMass – November 22, 2016

- UMass settled potential violations of the HIPAA Privacy and Security Rules. The settlement includes a corrective action plan and a monetary payment of $650,000, which is reflective of the fact that the University operated at a financial loss in 2015.
- On June 18, 2013, UMass reported that a workstation in its Center for Language, Speech, and Hearing was infected with a malware program, which resulted in the impermissible disclosure of the ePHI of 1,670 individuals. The University determined that the malware was a generic remote access Trojan that infiltrated their system, providing impermissible access to ePHI, because UMass did not have a firewall in place.
- OCR's investigation found that UMass had failed to designate all of its health care components when hybridizing, incorrectly determining that while its University Health Services was a covered health care component, other components, including the Center where the breach of ePHI occurred, were not covered components.
- Among other findings, UMass did not conduct an accurate and thorough risk analysis until September 2015.

St. Joseph Health - October 18, 2016

- St. Joseph Health (SJH) has settled potential violations of the HIPAA Privacy and Security Rules following the report that files containing ePHI were publicly accessible through internet search engines from 2011 until 2012. SJH has paid a settlement amount of $2,140,500 and will adopt a comprehensive corrective action plan.
- SJH reported that certain files it created for its participation in the meaningful use program were publicly accessible on the internet from 2011-2012, via Google and possibly other internet search engines. The server SJH purchased to store the files included a file sharing application whose default settings allowed anyone with an internet connection to access them. Upon implementation of this server and the file sharing application, SJH did not examine or modify it. As a result, the public had unrestricted access to PDF files containing the ePHI of 31,800 individuals.
- SJH has agreed to a corrective action plan that requires the organization to conduct an enterprise-wide risk analysis, develop and implement a risk management plan, revise its policies and procedures, and train its staff on these policies and procedures.

Policy Updates

Cloud Computing Guidance October 7, 2016

- OCR has issued important new guidance to assist organizations, including cloud service providers (CSPs), in understanding their HIPAA obligations.
- The guidance presents key questions and answers to assist HIPAA-regulated CSPs and their customers in understanding their responsibilities under the HIPAA Rules when they create, receive, maintain, or transmit electronic protected health information using cloud products and services.
- You may find the new guidance on OCR's website at: http://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
- OCR's FAQs on this topic may be found under "Business Associates – Cloud Computing" at: http://www.hhs.gov/hipaa/for-professionals/faq/business-associates

HIPAA and the FTC Act October 21, 2016

- OCR and the FTC have issued joint guidance reminding HIPAA covered organizations that they also must comply with the Federal Trade Commission (FTC) Act
- The guidance reinforces that if you share health information, it's not enough to simply consider the HIPAA Privacy Rule. You also must make sure your disclosure statements are not deceptive under the FTC Act.
- Find the new guidance at https://www.ftc.gov/tips-advice/business-center/guidance/sharing-consumer-health-information-look-hipaa-ftc-act

Cybersecurity Newsletters

- **October 2016:** ***Mining More than Gold***
  - Reviews vulnerabilities of file transfer protocols, a type of data storage used to used to transfer computer files on a computer network
  - Alerts HIPAA covered entities of a malware variant called Mal/Miner-C (also known as PhotMiner) which tricks users by copying files to public folders that resemble a standard Microsoft folder icon.
  - Some best practices include limiting user access; performing regular physical audits and checks for unauthorized equipment; performing detailed network-traffic analysis; and keeping anti-virus and anti-malware software up to date;

- **November 2016:** ***What Type of Authentication is Right for you?***
  - Reviews best practices and recommended methods of authentication, depending on the results of risk analyses, including single-factor and multi-factor authentication

What’s to Come

- 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

- OCR has begun sending document request packages to business associates this week as we continue with Phase 2 of our audit program.
- An additional email will be sent to these entities asking them to participate in an opening meeting webinar on December 6th from 11am to 1pm.
- We continue to update our audit web pages regularly where our Phase 2 audit protocol is posted, announcements are shared, and frequently asked questions are addressed.
- http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html

Questions?

http://www.hhs.gov/hipaa

Join us on Twitter @hhsocr