2016: YEAR OF THE HIPAA AUDIT

Presentation by:
Patrick Ho, USC Pharm D. Candidate of 2017
Preceptor:
Craig Stern, PharmD, MBA, RPh, FASCP, FASHP, FICA, FLMI, FAMCP
HIPAA 2016: An Overview

- Review HIPAA
- Digitization of Health Records
- Breaches in Healthcare Data
- Cybersecurity
- Audit enforcement
- Compliance programs
What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996
- Establishes national standards to protect individuals’ medical records and other personal health information (PHI)
- Minimum Necessary Requirement
  - Using only the minimum necessary health information to satisfy a particular purpose or function
- Patients’ Right to Privacy
  - Privacy and freedom from intrusions regarding personal affairs
Who handles personal health info?

- **Treatment**
  - *Doctors & other healthcare providers*

- **Payment**
  - *Health insurance*

- **Organizations**
  - *Drug utilization review / data review*
  - *Case management*
What’s New?
Digitization of Health Records

- Obama administration
- Fully integrated Electronic Health Records (EHR) system
- Breaking down silos in healthcare
- Huge jump in healthcare efficiency and effectiveness
- But...
  - Slow to adopt electronic records
  - Lack of security infrastructure
What’s New?
The Value of Health Data

■ Hackers now prefer health data
■ Large market for health insurance fraud $\rightarrow$ identity theft
■ 10-20 times more than credit cards on the black market
■ Credit cards can be cancelled, medical records are permanent
■ EHR takes twice as long as normal identity theft to detect
■ The majority of medical identity theft victims will find themselves paying around $13,500 to resolve identity theft issues.
■ Victims hold providers responsible for their information

2. https://hipaashealthlaw.foxrathschild.com/2015/03/articles/privacy/hacked-health-records-prized-for-their-black-market-value/
Data Breaches in Healthcare

- 8 of the 10 largest provider data breaches occurred in 2015
- Almost 90% of the health-care organizations surveyed had a data breach in the past two years
- Recent wave of ransomware attacks
- Estimated annual cost of $6.2 billion
- The U.S. Department of Health and Human Services (HHS) announced that it will launch HIPAA audits early 2016 in order to be more proactive in HIPAA enforcement.

1. https://hipaahealthlaw.foxrothschild.com/2015/03/articles/privacy/hacked-health-records-prized-for-their-black-market-value/
Encryption

- **Encrypt all electronic information** using the NIST (National Institute of Standards and Technology) standard.

- Use technology (e.g. enterprise-wide anti-virus) to **detect and prevent unauthorized use and transmission** of electronic data. Purchase cyber insurance for your organization.

- **Self-assess for gaps in privacy and security** and continually improve processes, procedures, technology, and staff education.

- **Train and document your educational efforts** for both new and existing staff members. Staff members should take regularly scheduled refresher courses followed by assessments that reflect real-life situations.

Mitigating Costs

- HIPAA security risk assessments
  - Data breaches ➔ millions of dollars in settlements
- Encryption
  - Stolen unencrypted laptops automatically presumes a data breach ➔ hundreds of thousands of dollars in settlements
- Audit penalties are expensive

http://complianceandethics.org/hipaa-compliance-what-you-need-to-know-for-2016/
Office of Civil Rights (OCR) Audits

- OCR Phase I Audit results
  - 2/3s of entities lacked complete & accurate risk assessment

- OCR Phase II Audit – 2016
  - Providers will be randomly selected (including Hospitals, healthcare providers, health plans, business associates)
  - Includes “small” providers – those with fewer than 15 physicians
  - Greater focus on encryption and decryption
HIPAA: Why comply?

- Not just a binder on the shelf
- Not optional – Everyone is expected to comply
- Compliance is a part of doing business
- Compliance is a means to adapt to ever-changing mandates and industry threats
- US Sentencing Guidelines provide leniency for entities that adopt effective compliance programs (lesser penalties for violations)
HIPAA Compliance
Policies and procedures to prevent, detect, contain, and correct security violations

- INVENTORY PHI storage assets, ASSESS risks & vulnerabilities
- Implement SECURITY MEASURES to reduce risks & vulnerabilities
- Establish SANCTIONS against members who fail to comply
- REGULARLY REVIEW records
- UPDATE POLICIES in response to changing environment
Take Home Points

■ Technology in healthcare is growing fast, but electronic security isn’t.
■ Be cybersecure! Know where your encryption stands.
■ HIPAA compliance is mandatory. Prepare now in case your organization is selected for audit.
■ Encryption saves money!
■ Strong data security protects your patients!
Questions?