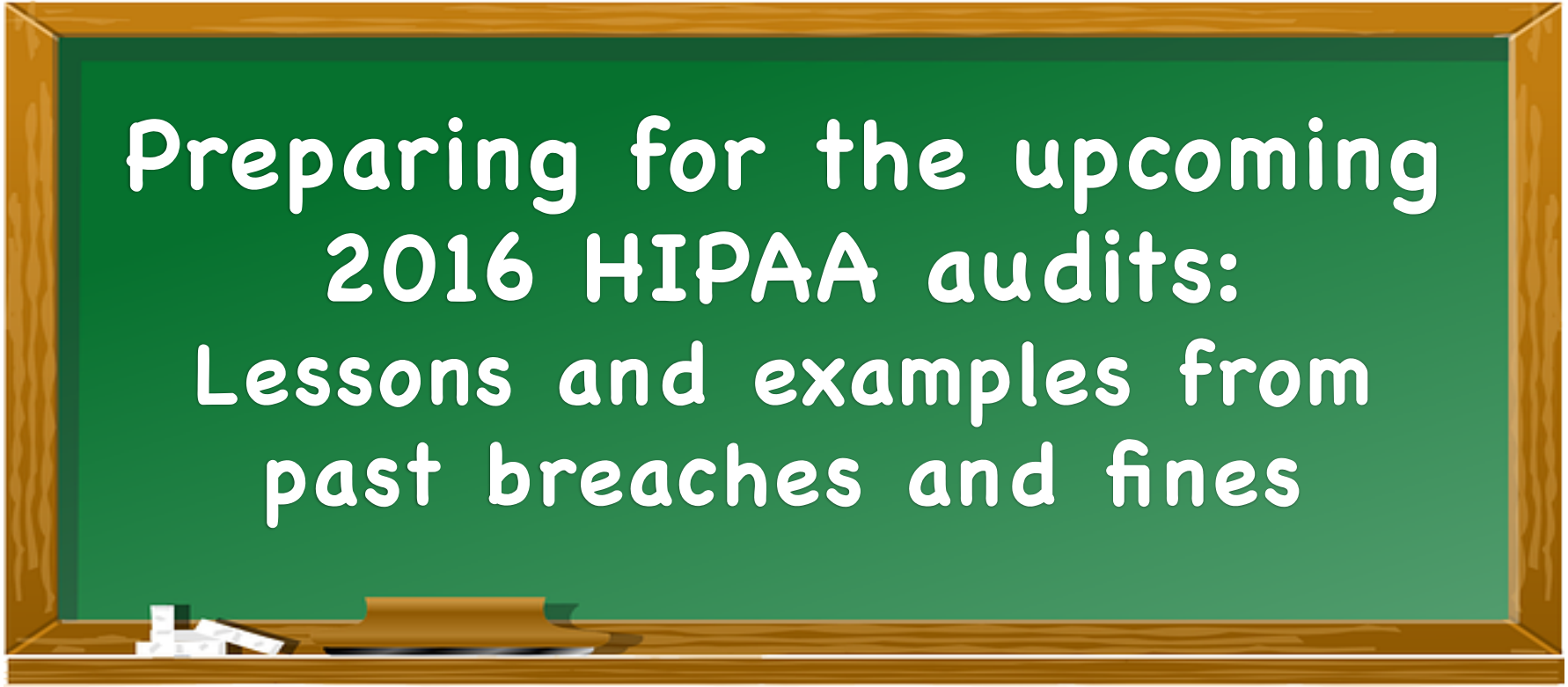
Preparing for the upcoming 2016 HIPAA audits: Lessons and examples from past breaches and fines



Your Presenters

Robert Grant

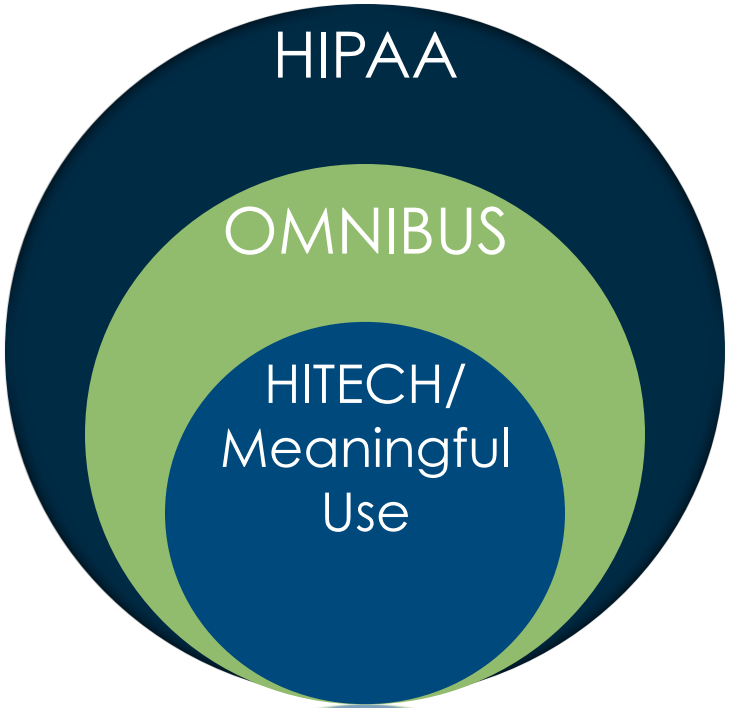
- Co-Founder and Chief Strategy Officer of Compliancy Group
- Over 15 years of experience in the compliance industry
- Assessed hundreds of healthcare entities for both Privacy and Security assessments
- Consulted with: **Principal Financial Group**, **United Healthcare**, **Molina Healthcare**, **Kaiser Permanente**

David Schulz

- CEO of Cyber Risk Associates
- Certified Information Privacy Professional & HIPAA Compliance specialist (CIPP; CHP)
- Nonprofit leadership posts at **SMU**, **UT-Dallas**, **Austin College**, **SPCA of Texas** and **Foundation of Americas Blood Centers**;
- IAPP San Antonio Knowledge Net chapter chair
- Writings appear in: American History Magazine, Dallas Morning News, D Magazine, Variety, San Antonio Express News and upcoming San Antonio Medicine magazine, "Texas Privacy: HIPAA On Steroids."

HIPAA & HITECH

- HIPAA
  - Protect patient confidentiality while furthering innovation and patient care.
- Omnibus
  - Business Associates must protect PHI.
- HITECH/Meaningful Use
  - Accelerate adoption of EHR(electronic Health records).
- Penalties or Incentives for adherence



The Seven Fundamental Elements of an Effective Compliance Program

Compliance according to HHS:

1. Implementing written policies, procedures and standards of conduct.
2. Designating a compliance officer and compliance committee.
3. Conducting effective training and education.
4. Developing effective lines of communication.
5. Conducting internal monitoring and auditing.
6. Enforcing standards through well-publicized disciplinary guidelines.
7. Responding promptly to detected offenses and undertaking corrective action.

*Source HHS & OIG

Trends in HIPAA

HIPAA compliance as a **differentiator**

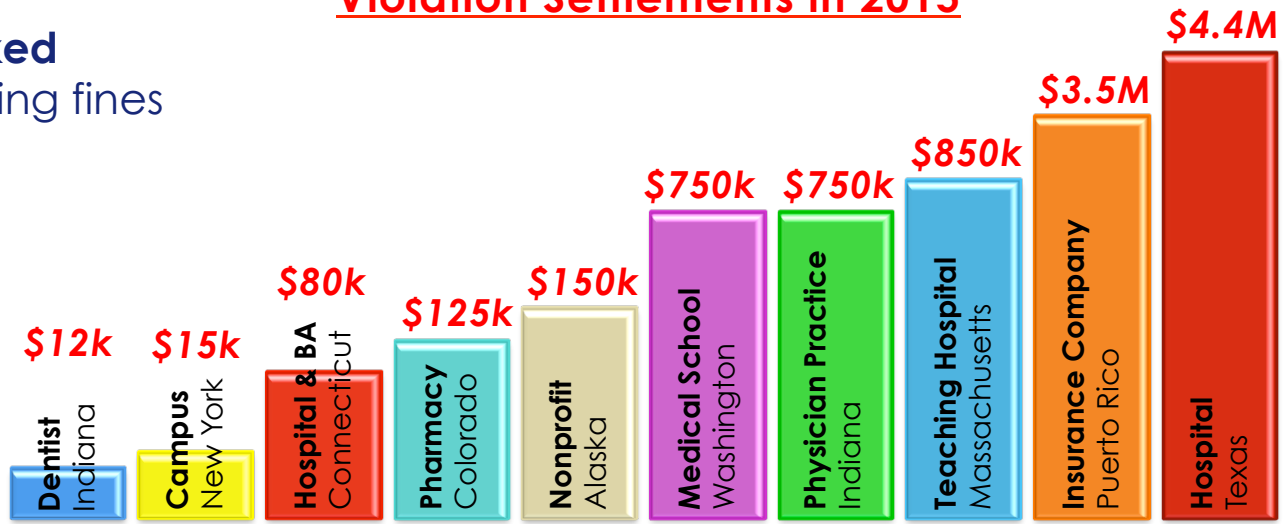
- **Fitbit Inc.** – announces its HIPAA compliance, stock price soared (26%)

- **THREE** Prison Sentences
- Medical License **Revoked**
- **Attorney Generals** levying fines

1 in 4 Americans

Affected by Anthem Breach

Violation Settlements in 2015



2016 Mandatory Audits: Phase 2

- BOTH Covered Entities and Business Associates will be audited
- OCR (Office of Civil Rights) audit request sent 2 weeks prior to audit
- Stricter audit protocols
- Vendor to carry out audits has been selected – FCi Federal

Insurance Holding Company

- Triple-S Management Corporation (Puerto Rico)
- Several breach notices
- *Failure to conduct thorough risk analysis, failure to implement appropriate safeguards*
- Settlement: **$3.5 MILLION and 3-year Corrective Action Plan** (11/30/15)
  - ***"This case sends an important message for Covered Entities not only about compliance with the requirements of the Security Rule, including risk analysis, but compliance with the requirements of the Privacy Rule (business associate agreements and the minimum necessary use)." - OCR Director Jocelyn Samuels***

http://www.hhs.gov/about/news/2015/11/30/triple-s-management-corporation-settles-hhs-charges.html

Laptop Theft

- Cancer Care Group, P.C. (Indiana)
- A laptop stolen from an employee's car
- *The lack of **comprehensive risk analysis** and device and media control policy lead to a steep penalty*
- Settlement: **$775,000 and 3-year Corrective Action Plan** (9/2/15)

http://www.hhs.gov/about/news/2015/09/02/750.000-dollar-hipaa-settlement-emphasizes-the-importance-of-risk-analysis-and-device-and-media-control-policies.html

Unencrypted Laptop Theft

- Concentra Health Services (Missouri)
- Unencrypted laptop stolen from physical therapy facility
- *Failed to implement necessary policies and procedures or remediation efforts to address threats and vulnerabilities*
- Settlement: **$1,725,220 and 2-year Corrective Action Plan** (4/22/14)

http://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html

Unencrypted Laptop Theft

- QCA Health Plan, Inc. (Arkansas)
- Unencrypted laptop stolen from workforce member's car
- *Failed to implement necessary policies and procedures or conduct a security risk analysis*
- Settlement: **$250,000 and 2-year Corrective Action Plan** (4/22/14)

http://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html

Data Access Controls

- NY Presbyterian Hospital & Columbia University (New York)
- ePHI inadvertently made accessible through internet search when a personally owned computer server was to be attempted to be deactivated
- *Failed to conduct SRA or complied with their own data security policies and procedures*
- Settlement: **$3.3 MILLION (NYP) and $1.5 MILLION (Columbia) and 3-year Corrective Action Plans** (5/7/14)

http://www.hhs.gov/about/news/2014/05/07/data-breach-results-48-million-hipaa-settlements.html

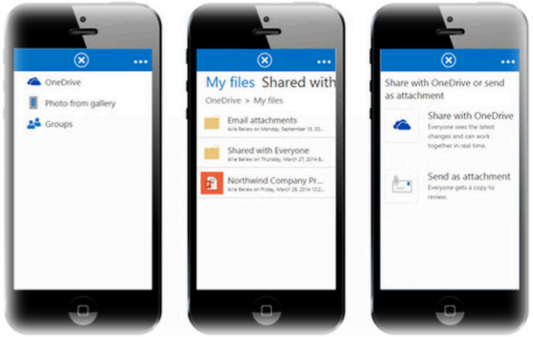
County Government

- Skagit County (Washington)
- ePHI inadvertently moved to a publicly accessible server
- *Widespread non-compliance with HIPAA Privacy, Security, and Breach Notification Rules*
- Settlement: **$215,000 and 3-year Corrective Action Plan** (3/7/14)

http://www.hhs.gov/about/news/2014/03/07/county-government-settles-potential-hipaa-violations.html

File-Sharing Apps

- St. Elizabeth's Medical Center (Mass.)
- Used internet-based file sharing app to store ePHI
- *Failed to timely identify and respond to a known security incident, mitigate the harmful effects, or document the security incident and its outcomes*
- Settlement: **$218,400 and 1-year Corrective Action Plan** (6/10/15)



http://www.beckershospitalreview.com/healthcare-information-technology/st-elizabeth-s-to-settle-hipaa-violation-for-218-000.html

Email Malware

- University of Washington Medicine (Washington)
- Employee opened a phishing email containing malware
- *Although UWM had policies requiring up-to-date risk assessments and implemented safeguards UWM did not ensure its affiliates were properly conducting their risk assessments and responding to risks and vulnerabilities*
- Settlement: **$750,000 and 2-year Corrective Action Plan** (12/14/15)

http://www.hhs.gov/about/news/2015/12/14/750000-hipaa-settlement-underscores-need-for-organization-wide-risk-analysis.html

Physical Security

- Lahey Hospital and Medical Center (Mass.)
- Portable CT scanner stolen from unlocked room overnight
- *Failure to conduct a thorough risk assessment for all ePHI, failure to physically safeguard workstation with ePHI, failure to implement unique user names to identify and track users, and failure to document workstation activity.*
- Settlement: **$850,000 and 3-year Corrective Action Plan** (11/24/15)

Pharmacy

- Cornell Prescription Pharmacy (Colorado)
- Disposed of unsecured documents in an unlocked open container
- *Failure to implement written policies and procedures, and filed to provide training to its workforce*
  - ***"Regardless of size, organizations cannot abandon protected health information or dispose of it in dumpsters or other containers that are accessible by the public or other unauthorized persons." - OCR Director Jocelyn Samuels.***
- Settlement: **$125,000 and 2-year Corrective Action Plan** (11/24/15)

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/cornell/cornell-press-release/index.html

Medical Records Dumped

- Parkview Health System (Indiana/Ohio)
- Employees left boxes of medical records on a physician's driveway unattended and accessible to unauthorized persons
- *Failed to protect PHI during its transfer and disposal*
- Settlement: **$800,000 and 2-year Corrective Action Plan** (11/24/15)

http://www.hhs.gov/about/news/2014/06/23/800000-hipaa-settlement-in-medical-records-dumping-case.html

Dentist

- Dr. Joseph Beck (Indiana)
- *Mishandled medical records containing sensitive information of more than 5,600 patients.*
- Settlement: **$12,000 license to practice dentistry permanently revoked** (1/9/15)

http://kokomoperspective.com/kp/state-settles-with-former-dentist-accused-of-dumping-patient-files/article_3a5dbbfc-9831-11e4-b5ee-2fb4d5ff867a.html

Practice Sued By Patients

- Midwest Women's Healthcare Specialists (Missouri)
- Improperly disposed PHI of 1,532 patients
- Class-action lawsuit brought by patients
- Civil Settlement: **$400,000** (12/4/14)
- HHS Fine/Settlement: **$$$$$$ (TBD)**

http://healthitsecurity.com/news/phi-exposure-case-1500-patients-settled

Avoidable Breach

- Nonprofit org. - ACMHS (Alaska)
- Malware caused breach of unsecured ePHI
- *"ACMHS had adopted policies and procedures in **2005**, but these policies and procedures were not followed and/or updated."*
- ACMHS could have **avoided** the breach (and not be subject to the settlement agreement), if it had followed its own policies and procedures
- Settlement: **$150,000 and 2-year Corrective Action Plan** (1/5/15)

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/acmhs/index.html

State Attorney Levying Fine

- University of Rochester Medical Center (NY)
- A former employee (nurse practitioner) obtain a patient list (including addresses and diagnoses) without the patients' consent and gave the list to her new employer
- New York State Attorney fine: **$15,000 provide (policies/procedures, training) to the Attorney General** (12/4/15)

http://cooleyhealthbeat.com/2015/12/09/university-of-rochester-medical-center-reaches-agreement-to-settle-alleged-hipaa-breach/

Business Associate

- Hartford Hospital and EMC Corp(Connecticut)
- This action comes after an unencrypted laptop containing PHI were stolen from the home of an EMC employee. EMC was a business associate to Hartford Hospital.
- Connecticut State Attorney General: **$90,000 collectively between EMC Corp and Hartford Hospital** (11/10/15)

http://www.lexology.com/library/detail.aspx?g=412dda6f-3866-496a-b628-151c34fef36a

Lessons Learned

- OCR enforcement on the rise, penalties are high
- While larger entities are at higher risk, smaller entities are also at risk
- Mandatory breach notifications sent to OCR trigger investigations
- Covered entities are responsible for their workforce as well as their business associates
- Paper records must be safeguarded as well!
- State Attorney Generals can levy fines

The Seven Fundamental Elements of an Effective Compliance Program

Compliance according to HHS:

1. Implementing written policies, procedures and standards of conduct.
2. Designating a compliance officer and compliance committee.
3. Conducting effective training and education.
4. Developing effective lines of communication.
5. Conducting internal monitoring and auditing.
6. Enforcing standards through well-publicized disciplinary guidelines.
7. Responding promptly to detected offenses and undertaking corrective action.

*Source HHS & OIG

The Problems With Industry Solutions

A Risk Assessment is **NOT** enough!

- Typical solutions - Policy, Procedures, and Training templates and/or a Security Risk Assessment.
- Only address pieces of compliance and require additional costs for additional components.
- Leads to cumbersome internal efforts, outside resources, and no assurance of compliance.

Total Cost of Compliance
(single location practice/organization)

$8,000+ per year

Solving The HIPAA Compliance Puzzle

- The pieces of HIPAA compliance.
- Every piece must be completed annually or as the regulations change.
- Missing even one piece can result in fines or loss of reputation.

Compliance Questions?

For more information, contact:

Bob Grant
855.854.4722 ext 502
bob@compliancygroup.com

David Schulz
210.281.8151
DAS@cyberriskassociates.com