2016 HIPAA Year In Review: Audits, Fines, and Enforcement Trends

HHS Wall of Shame

Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
TriHealth, Inc.	OH	Healthcare Provider	1126	01/19/2017	Unauthorized Access/Disclosure	Network Server, Paper/Films
Escambia County Alabama Community Hospitals, Inc. D/B/A Atmore Community Hospital	AL	Healthcare Provider	1090	01/12/2017	Unauthorized Access/Disclosure	Electronic Medical Record
Office of Dr. David Elbaum	CA	Healthcare Provider	500	01/09/2017	Theft	Paper/Films
Complete Wellness	MD	Healthcare Provider	600	01/06/2017	Loss	Other Portable Electronic Device
American Urgent Care Center, PSC	KY	Healthcare Provider	822	01/05/2017	Theft	Other
MetroPlus Health Plan	NY	Health Plan	808	01/03/2017	Unauthorized Access/Disclosure	Other
Bryan Myers, MD PC, Ashley DeWitt, DO PC, Michael Nobles, MD PC	TN	Healthcare Provider	13150	12/30/2016	Hacking/IT Incident	Network Server
State of New Hampshire, Department of Health and Human Services	NH	Healthcare Provider	15000	12/30/2016	Hacking/IT Incident	Desktop Computer
Horizon Healthcare Services Inc. doing business as Horizon Blue Cross Blue Shield of New Jersey and its affiliates	NJ	Health Plan	55700	12/30/2016	Unauthorized Access/Disclosure	Paper/Films
PathGroup	TN	Health Plan	1443	12/29/2016	Unauthorized Access/Disclosure	Other
PrimeWest Health	MN	Health Plan	2441	12/29/2016	Hacking/IT Incident	Network Server
Susan M Hughes Center	NJ	Healthcare Provider	11400	12/27/2016	Hacking/IT Incident	Network Server
Brandywine Pediatrics, P.A.	DE	Healthcare Provider	26873	12/23/2016	Hacking/IT Incident	Network Server
Waiting Room Solutions Limited Liability Limited Partnership	NY	Business Associate	700	12/23/2016	Unauthorized Access/Disclosure	Email
Stephen J. Helvie, M.D.	CA	Healthcare Provider	2013	12/22/2016	Theft	Paper/Films
ADVANTAGE Health Solutions	IN	Health Plan	2387	12/22/2016	Hacking/IT Incident	Network Server
Community Health Plan of Washington	WA	Health Plan	381504	12/21/2016	Hacking/IT Incident	Network Server, Other
Henry County Health Department	OH	Healthcare Provider	574	12/21/2016	Theft	Electronic Medical Record, Email, Laptop, Paper/Films
Desert Care Family and Sports Medicine	AZ	Healthcare Provider	500	12/20/2016	Hacking/IT Incident	Network Server
Alliant Health Plans, Inc.	GA	Health Plan	1042	12/20/2016	Hacking/IT Incident	Network Server

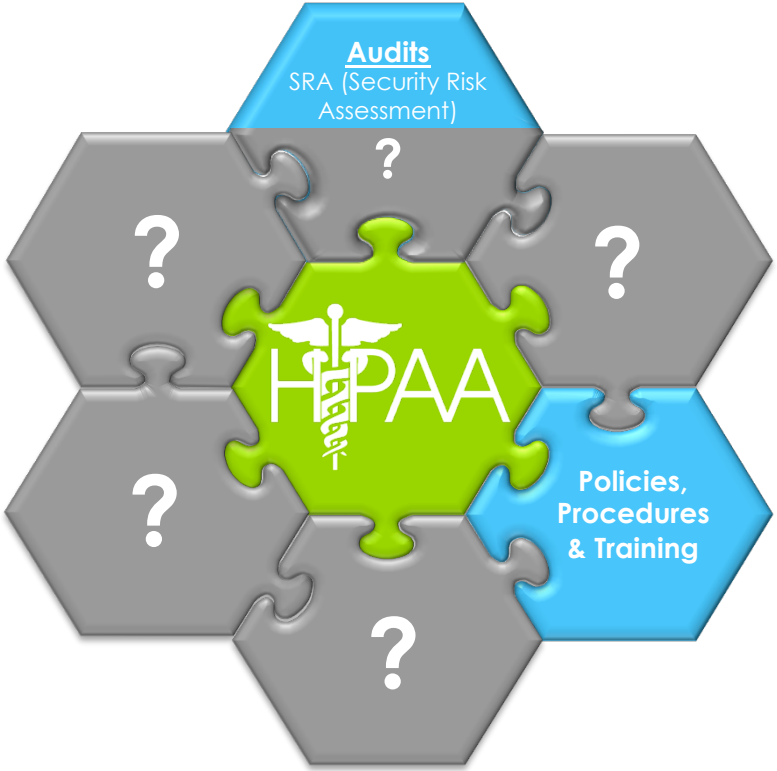
Based on HHS Breach Portal: Breaches Affecting 500 or More Individuals, "Type of Breach" https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Why Should I Worry About HIPAA?

HIPAA is the Law

- **HIPAA is confusing**
  - SRA (Security Risk Assessment)
  - Policies & Procedures
  - Training
- **Current market solutions only address *pieces* of compliance**
- **Enforcement is on the rise ↑**
  - Record fines levied: **$24 Million** in 2016
  - Three prison sentences
  - Medical license revoked
  - State Attorney General levying fines

FAIL



HIPAA Enforcement

- Settlements in 2016 totaled **more than any year prior: $24 million**

*"All too often we see covered entities with a **limited risk analysis**"*

*"Organizations must have in place compliant **business associate agreements** as well as an accurate and thorough risk analysis"*

*"We take seriously **all complaints filed by individuals**, and will seek the necessary remedies to ensure that patients' privacy is fully protected."*

- Jocelyn Samuels, Director of OCR

- **Three** Prison Sentences
- Medical License **Revoked**
- **State Attorney General** levying fines

* $23,979,800 FY 2016, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

What is HIPAA?

Compliance vs. Security

- Fines vs. Risk

HIPAA/HITECH

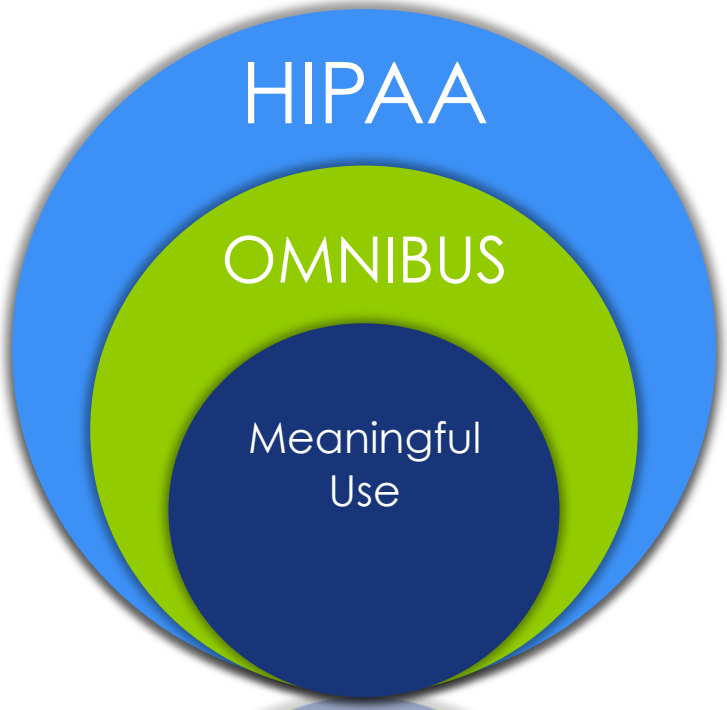
- Protect patient confidentiality while furthering innovation and patient care
- Privacy Rule and Security Rule

Meaningful Use

- Accelerate adoption of EHR (electronic Health records)

Omnibus

- Business Associates must be HIPAA compliant
- Covered Entities must have BAAs
  - Conduct Due Diligence
- Breach Notification Rule



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

Avoidable Breach

- Who: **Nonprofit** org. - Anchorage Community **Mental Health Services** (ACMHS)
- What: **Malware** caused breach of unsecured ePHI
- Why: ACMHS could have **avoided** the breach (and not be subject to the settlement agreement), if it had followed its own policies and procedures
- Ruling: **$150,000 & CAP** (1/5/15)

*"ACMHS had adopted policies and procedures in **2005**, but these policies and procedures were **not followed and/or updated**."*

http://www.healthcareitnews.com/news/hhs-slaps-group-150k-hipaa-breach-bill

Improper Disclosure Of PHI

- Who: Feinstein Institute for **Medical Research**
- What: **Laptop stolen from car contained** (13,000 PHI) of research participants. **Password-protected but not encrypted**
- Why: Failed to reasonably safeguard PHI;
  - **Lacked policies & procedures** for ePHI access
  - **Failed to implement policies and procedures** to safeguard ePHI
- Ruling: **$3.9 Million & CAP** (3/17/16)

*"**Research institutions** subject to HIPAA must be held to the **same compliance standards as all other HIPAA-covered entities**," said OCR Director Jocelyn Samuels. "For individuals to trust in the research process and for patients to trust in those institutions, they must have some assurance that their information is kept private and secure."*

http://www.crainsnewyork.com/article/20160318/ECONOMY/160319845/the-feinstein-institute-for-medical-research-pays-3-9-million-to-settle-data-breach-one-of-the-largest-sums-ever-paid

The Need For BAAs

- Who: Raleigh **Orthopaedic** Clinic(North Carolina)
- What/Why: 17,300 patients affected
  - Handed over PHI (**X-ray films**) to potential business partner without first executing a **business associate agreement**.
- Settlement: **$750,000 & CAP** (4/20/16)

*"HIPAA's obligation on covered entities to obtain **business associate agreements** is more than a mere check-the-box paperwork exercise," said Jocelyn Samuels, Director of OCR. "It is critical for entities to know to whom they are handing PHI and to obtain assurances that the information will be protected."*

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/raleigh-orthopaedic-clinic-bulletin/index.html

Importance of BAA & Complete Risk Analysis

- Who: North Memorial Health Care of Minnesota
- What: **Laptop theft**, 6,497 patient records
- Why: No **BAA** with Billing firm;
  - **Failed to complete a risk analysis** to address all potential risks and vulnerabilities to ePHI
- Settlement: **$1.55 Million & CAP** (3/16/16)

"Two major cornerstones of the HIPAA Rules were overlooked by this entity," said Jocelyn Samuels, Director of OCR. "Organizations must have in place compliant ***Business Associate Agreements*** *as well as an* ***accurate and thorough risk analysis*** *that addresses their enterprise-wide IT infrastructure.*

http://www.hhs.gov/about/news/2016/03/16/155-million-settlement-underscores-importance-executing-hipaa-business-associate-agreements.html

Risk Analysis is NOT Enough

- Who: OHSU (Oregon Health & Science University)
- What: Reports of **unencrypted laptops, stolen unencrypted thumb drive**, 1,361 patient records
- Why: Conducted **SIX** risk analysis in (2003, 2005, 2006, 2008, 2010, 2013) but did not address the widespread vulnerabilities**.** Also, lacked **policies & procedures.** Lack of **BAA.**
- Settlement: **$2.7 Million & CAP** (7/18/16)

*"From well-publicized large scale breaches and findings in their own risk analyses, OHSU **had every opportunity to address security** management processes that were insufficient. Furthermore, OHSU should have addressed the lack of a business associate agreement before allowing a vendor to store ePHI," said OCR Director Jocelyn Samuels. "This settlement underscores the importance of leadership engagement and why it is so critical for the C-suite to **take HIPAA compliance seriously**."*

http://www.hhs.gov/about/news/2016/07/18/widespread-hipaa-vulnerabilities-result-in-settlement-with-oregon-health-science-university.html

Unauthorized Patient Testimonials

- Who: Complete P.T. Pool & Land **Physical Therapy**
- What: **Posted patient testimonials** (including names/ photos) on website without authorization.
- Why: Failed to reasonably safeguard PHI;
  - **Impermissibly disclosed PHI without authorization;**
  - **Failed to implement policies and procedures** to comply with HIPAA regarding authorization
- Ruling: **$25,000 & CAP** (2/16/16)

*"The **HIPAA Privacy Rule gives individuals** important **controls** over whether and how their protected health information is **used and disclosed for marketing** purposes," said OCR Director Jocelyn Samuels. "With limited exceptions, the Rule requires an individual's **written authorization** before a use or disclosure of his or her protected health information can be made for marketing."*

http://www.healthcareitnews.com/news/physical-therapist-pay-25000-over-unauthorized-patient-testimonials

First Business Associate Penalty

- Who: Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS), **IT services for nursing facilities**
- What: **iPhone theft** (412 PHI)
- Why: Device was **unencrypted** and **not password protected**;
  - **Lack of policies & procedures** for removal of PHI devices
  - Lack of policies & procedures to address **incidents**
  - **No risk analysis or risk management plan**
- Settlement: **$650,000 & CAP** (6/29/16)

*"**Business associates must implement** the protections of the **HIPAA Security Rule** for the electronic protected health information they create, receive, maintain, or transmit from covered entities," said Office for Civil Rights (OCR) Director Jocelyn Samuels. "This includes an **enterprise-wide risk analysis** and corresponding risk management plan, which are the cornerstones of the HIPAA Security Rule."*

http://www.hhs.gov/about/news/2016/03/16/155-million-settlement-underscores-importance-executing-hipaa-business-associate-agreements.html

Largest Settlement To Date

- Who: Advocate Health Care
- What: **Breach Notification Reports** submitted (4 Mill. PHI)
- Why: Fail to:
  - **Conduct thorough Risk Analysis**
  - **Implement policies & procedures**
  - **Obtain proper BAAs**
  - **Reasonably safeguard unencrypted laptop**
- Settlement: **$5.55 Million & CAP** (8/4/16)

*"We hope this settlement sends a strong message to covered entities that they must engage in **a comprehensive risk analysis and risk management** to ensure that individuals' ePHI is secure," said OCR Director Jocelyn Samuels. "This includes implementing **physical, technical, and administrative** security measures sufficient to reduce the risks to ePHI in all physical locations and on all portable devices to a reasonable and appropriate level."*

https://www.hhs.gov/about/news/2016/08/04/advocate-health-care-settles-potential-hipaa-penalties-555-million.html

Hybrid Entity Fined

- Who: UMass (University of Massachusetts Amherst)
- What: **Malware program** (1,670 PHI), no firewall in place
- Why: **Failed to designate health care components**;
  - Did not conduct accurate and thorough **Risk Analysis**
  - Failed to implement **technical measures**
- Settlement: **$650,000 & CAP** (11/22/16), reflecting the fact that UMass showed financial loss in 2015

*"HIPAA's security requirements are an important tool for protecting both patient data and business operations against threats such as malware," said OCR Director Jocelyn Samuels. "Entities that elect **hybrid status must properly designate their health care components** and ensure that those components are in compliance with HIPAA's privacy and security requirements."*

https://www.hhs.gov/about/news/2016/08/04/advocate-health-care-settles-potential-hipaa-penalties-555-million.html

OCR Is Ready For Court

- Who: Lincare (**Respiratory Care**)
- What: **Employee left behind documents** (278 PHI) after moving. **Lincare claimed it did not violate HIPAA**. Admin Law Judge **ruled in favor of OCR** for civil monetary penalty.
- Why: **Inadequate policies & procedures;**
  - **Minimal action to correct after complaint**
- Ruling: **$239,800 & CAP** (2/3/16)

*"While OCR prefers to resolve issues through voluntary compliance, this case shows that **we will take the steps necessary, including litigation**, to obtain adequate remedies for violations of the HIPAA Rules," said OCR Director Jocelyn Samuels. "The decision in this case validates the findings of our investigation.*

http://www.modernhealthcare.com/article/20160209/NEWS/160209856

No Filming Allowed

- Who: NYP(New York Presbyterian Hospital)
- What: **Unauthorized filming of two patients for a TV show (NY Med)**
- Why: **Failed to safeguard PHI;**
  - **Allowed an environement where PHI could not be protected.**
- Ruling: **$2.2 Million & CAP** (4/21/16)

"This case sends an important message that **OCR will not permit covered entities to compromise their patients' privacy** by allowing news or television crews to film the patients without their authorization," said Jocelyn Samuels, OCR's Director. "**We take seriously all complaints** filed by individuals, and will seek the necessary remedies to ensure that patients' privacy is fully protected."

https://www.hhs.gov/about/news/2016/04/21/unauthorized-filming-ny-med-results-22-million-settlement-new-york-presbyterian-hospital.html

Phase 2 Mandatory Audits

- 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
  - FCi Federal

Tardy Breach Notification = 1st Fine Of 2017

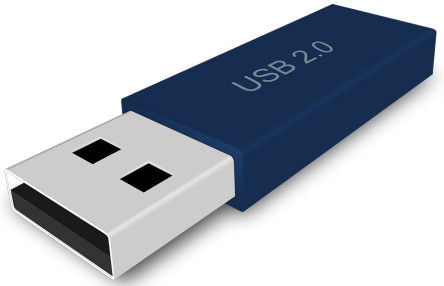
- Who: Presence Health
- What: **Missing paper schedules** (836 PHI)
- Why: **Failed to notify within 60 days** of discovery:
  - **Media outlets**
  - **OCR**
  - **Individuals affected**
- Settlement: **$475,000 & CAP** (1/9/17)

*"Covered entities need to have a clear policy and procedures in place to respond to the **Breach Notification Rule's timeliness requirements**" said OCR Director Jocelyn Samuels. "**Individuals need prompt notice of a breach** of their unsecured PHI so they can take action that could help mitigate any potential harm caused by the breach."*

https://www.hhs.gov/about/news/2017/01/09/first-hipaa-enforcement-action-lack-timely-breach-notification-settles-475000.html

PHI MUST Be Safeguarded

- Who: MAPFRE (Insurance Company of Puerto Rico)
- What: **USB drive stolen** (2,209 PHI)
- Why: **Failure to conduct Risk Analysis;**
  - Failure **to implement risk management plans**
  - Failure to deploy **encryption** on PHI devices
  - **Failed to implement/delayed implementing corrective measures**
- Settlement: **$2.2 Million & CAP** (1/18/17)



*"Covered entities must not only make assessments to safeguard ePHI, they must act on those assessments as well" said OCR Director Jocelyn Samuels. "OCR works tirelessly and collaboratively with covered entities to **set clear expectations and consequences**."*

https://www.hhs.gov/about/news/2017/01/18/hipaa-settlement-demonstrates-importance-implementing-safeguards-ephi.html

Solving The HIPAA Compliance Puzzle

Compliance Questions?

For more information, contact:

Compliancy Group

Marc Haskelson
President & CEO
855.854.4722 Ext 507
marc@compliancygroup.com

Compliancy Group
855.854.4722
info@compliancygroup.com