2016 HIPAA Year In Review: Audits, Fines, and Enforcement Trends
# HHS Wall of Shame


<table>
<thead>
<tr>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Covered Entity Type</th>
<th>Individuals Affected</th>
<th>Breach Submission Date</th>
<th>Type of Breach</th>
<th>Location of Breached Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Escambia County Alabama Community Hospitals, Inc. d/b/a Almore Community Hospital</td>
<td>AL</td>
<td>Healthcare Provider</td>
<td>1090</td>
<td>01/12/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Electronic Medical Record</td>
</tr>
<tr>
<td>Office of Dr. David Elbaum</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>500</td>
<td>01/08/2017</td>
<td>Theft</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Complete Wellness</td>
<td>MD</td>
<td>Healthcare Provider</td>
<td>800</td>
<td>01/06/2017</td>
<td>Loss</td>
<td>Other Portable Electronic Device</td>
</tr>
<tr>
<td>American Urgent Care Center, PSC</td>
<td>KY</td>
<td>Healthcare Provider</td>
<td>822</td>
<td>01/05/2017</td>
<td>Theft</td>
<td>Other</td>
</tr>
<tr>
<td>MetroPlus Health Plan</td>
<td>NY</td>
<td>Health Plan</td>
<td>808</td>
<td>01/03/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Other</td>
</tr>
<tr>
<td>Bryan Myers, MD PC, Ashley DeWitt, DO PC, Michael Nobles, MD PC</td>
<td>TN</td>
<td>Healthcare Provider</td>
<td>13150</td>
<td>12/30/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>State of New Hampshire, Department of Health and Human Services</td>
<td>NH</td>
<td>Healthcare Provider</td>
<td>15000</td>
<td>12/30/2016</td>
<td>Hacking/IT Incident</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>Horizon Healthcare Services Inc. doing business as Horizon Blue Cross Blue Shield of New Jersey and its affiliates</td>
<td>NJ</td>
<td>Health Plan</td>
<td>55700</td>
<td>12/30/2016</td>
<td>Unauthorized Access/Disclosure</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>PathGroup</td>
<td>TN</td>
<td>Health Plan</td>
<td>1443</td>
<td>12/29/2016</td>
<td>Unauthorized Access/Disclosure</td>
<td>Other</td>
</tr>
<tr>
<td>PrimeWest Health</td>
<td>MN</td>
<td>Health Plan</td>
<td>2441</td>
<td>12/29/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Susan M Hughes Center</td>
<td>NJ</td>
<td>Healthcare Provider</td>
<td>11400</td>
<td>12/27/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Brandywine Pediatrics, P.A.</td>
<td>DE</td>
<td>Healthcare Provider</td>
<td>28873</td>
<td>12/23/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Waiting Room Solutions Limited Liability Limited Partnership</td>
<td>NY</td>
<td>Business Associate</td>
<td>700</td>
<td>12/23/2016</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
</tr>
<tr>
<td>Stephen J. Hevick, M.D.</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>2013</td>
<td>12/22/2016</td>
<td>Theft</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>ADVANTAGE Health Solutions</td>
<td>IN</td>
<td>Health Plan</td>
<td>2387</td>
<td>12/22/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Community Health Plan of Washington</td>
<td>WA</td>
<td>Health Plan</td>
<td>381504</td>
<td>12/21/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server, Other</td>
</tr>
<tr>
<td>Henry County Health Department</td>
<td>OH</td>
<td>Healthcare Provider</td>
<td>574</td>
<td>12/21/2016</td>
<td>Theft</td>
<td>Electronic Medical Record, Email, Laptop, Paper/Films</td>
</tr>
<tr>
<td>Desert Care Family and Sports Medicine</td>
<td>AZ</td>
<td>Healthcare Provider</td>
<td>500</td>
<td>12/20/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Alliant Health Plans, Inc.</td>
<td>GA</td>
<td>Health Plan</td>
<td>1042</td>
<td>12/20/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
</tbody>
</table>
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
HIPAA Enforcement

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

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

“**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

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

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

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.
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.”

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."

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.”

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.

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.”

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."

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.”

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.”

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.”

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.”

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 environment 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.”

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."

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

- Audits
  - SRA (Security Risk Assessment), Administrative, Privacy
- Remediation Plans
- Business Associate Management
- Document Version, Employee Attestation & Tracking
- Incident Management & Remediation
- Policies, Procedures & Training
Compliance Questions?

For more information, contact:

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

Compliancy Group
855.854.4722
info@compliancygroup.com