Industry leading Education
Today’s Webinar
- 2017’s HIPAA Onsite Audits: What to Expect and How to Pass

Webinars
- Upcoming & past webinars:
  http://compliancy-group.com/webinar/
HIPAA Compliance Simplified

Agenda
- HIPAA Overview
- Common misunderstandings
- HIPAA Enforcement
- What causes a Audit?
- Real World Stories
- How do I protect my practice?
### 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>St. Joseph's Hospital and Medical Center</td>
<td>AZ</td>
<td>Healthcare Provider</td>
<td>623</td>
<td>02/13/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Electronic Medical Record</td>
</tr>
<tr>
<td>Benchak, Friedlander, Coplan &amp; Aronoff LLP</td>
<td>OH</td>
<td>Business Associate</td>
<td>1134</td>
<td>02/10/2017</td>
<td>Theft</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Family Medicine East, Chartered</td>
<td>KS</td>
<td>Healthcare Provider</td>
<td>8800</td>
<td>02/03/2017</td>
<td>Theft</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>Catalina Post-Acute Care and Rehabilitation</td>
<td>AZ</td>
<td>Healthcare Provider</td>
<td>2693</td>
<td>02/02/2017</td>
<td>Improper Disposal</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Jeffrey D. Rice, O.D., L.L.C.</td>
<td>OH</td>
<td>Healthcare Provider</td>
<td>1596</td>
<td>02/02/2017</td>
<td>Theft</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>VeriCo Health &amp; Wellness Plan</td>
<td>OH</td>
<td>Health Plan</td>
<td>955</td>
<td>01/31/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>WellCare Health Plans, Inc.</td>
<td>FL</td>
<td>Health Plan</td>
<td>2406</td>
<td>01/27/2017</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Shiel Sexton</td>
<td>IN</td>
<td>Health Plan</td>
<td>710</td>
<td>01/27/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Other</td>
</tr>
<tr>
<td>Synergy Specialists Medical Group, Inc / Jay S. Berman, DPM</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>569</td>
<td>01/27/2017</td>
<td>Hacking/IT Incident</td>
<td>Email</td>
</tr>
<tr>
<td>Princeton Pain Management</td>
<td>NJ</td>
<td>Healthcare Provider</td>
<td>4665</td>
<td>01/27/2017</td>
<td>Hacking/IT Incident</td>
<td>Desktop Computer, Electronic Medical Record</td>
</tr>
<tr>
<td>THE R.O.A.D.S. Foundation Inc. DBA R.O.A.D.S. Community Care Clinic</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>670</td>
<td>01/26/2017</td>
<td>Loss</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>MultiCare Health System</td>
<td>WA</td>
<td>Healthcare Provider</td>
<td>1249</td>
<td>01/26/2017</td>
<td>Hacking/IT Incident</td>
<td>Email</td>
</tr>
<tr>
<td>Roper St. Francis Healthcare</td>
<td>SC</td>
<td>Healthcare Provider</td>
<td>576</td>
<td>01/24/2017</td>
<td>Loss</td>
<td>Other Portable Electronic Device</td>
</tr>
<tr>
<td>Stephenville Medical &amp; Surgical Clinic</td>
<td>TK</td>
<td>Healthcare Provider</td>
<td>73000</td>
<td>01/23/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>Multnomah County</td>
<td>OR</td>
<td>Healthcare Provider</td>
<td>1700</td>
<td>01/20/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
</tr>
<tr>
<td>Wonderville For Health Innovation</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>3398</td>
<td>01/20/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Other Portable Electronic Device</td>
</tr>
<tr>
<td>Multicare Medical Center, Inc.</td>
<td>MI</td>
<td>Healthcare Provider</td>
<td>6197</td>
<td>01/20/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
</tr>
<tr>
<td>Associated Catholic Charities Incorporated</td>
<td>MD</td>
<td>Healthcare Provider</td>
<td>1148</td>
<td>01/20/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
</tr>
</tbody>
</table>

## 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>Massachusetts Eye and Ear Infirmary</td>
<td>MA</td>
<td>Healthcare Provider</td>
<td>1076</td>
<td>03/01/2010</td>
<td>Theft</td>
<td>Other</td>
</tr>
<tr>
<td>Children’s EyeCare NY</td>
<td>NY</td>
<td>Healthcare Provider</td>
<td>1090</td>
<td>02/22/2015</td>
<td>Theft</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>Eye Institute of Corpus Christi</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>43961</td>
<td>03/26/2016</td>
<td>Theft</td>
<td>Electronic Medical Record</td>
</tr>
<tr>
<td>EyeCare of Bartsville</td>
<td>OK</td>
<td>Healthcare Provider</td>
<td>4000</td>
<td>03/13/2015</td>
<td>Hacking/IT Incident</td>
<td>Desktop Computer, Network Server</td>
</tr>
<tr>
<td>Massachusetts Eye and Ear Infirmary</td>
<td>MA</td>
<td>Healthcare Provider</td>
<td>3084</td>
<td>04/20/2010</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Oakland Vision Services, PC</td>
<td>MI</td>
<td>Healthcare Provider</td>
<td>3000</td>
<td>05/03/2012</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Southeast Eye Institute, P.A. the Eye Associates of Pinellas</td>
<td>FL</td>
<td>Healthcare Provider</td>
<td>87314</td>
<td>05/03/2015</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>University of Houston for Uni College of Optometry</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>7000</td>
<td>05/08/2012</td>
<td>Hacking/IT Incident, Unauthorized Access/ Disclosure</td>
<td>Network Server</td>
</tr>
<tr>
<td>Silicon Valley Eyecare Optometry and Contact Lenses</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>40000</td>
<td>05/13/2010</td>
<td>Theft</td>
<td>Network Server</td>
</tr>
<tr>
<td>Associates in Eyecare, P.S.C.</td>
<td>KY</td>
<td>Healthcare Provider</td>
<td>971</td>
<td>05/16/2016</td>
<td>Theft, Unauthorized Access/ Disclosure</td>
<td>Laptop, Other Portable Electronic Device</td>
</tr>
<tr>
<td>Gulf Breeze Family Eyecare, Inc.</td>
<td>FL</td>
<td>Healthcare Provider</td>
<td>9626</td>
<td>05/17/2013</td>
<td>Theft, Unauthorized Access/ Disclosure</td>
<td>Desktop Computer, Electronic Medical Record, Email, Network Server, Paper/Prints</td>
</tr>
<tr>
<td>Cefalu Eye-Tech of Green, Inc.</td>
<td>CH</td>
<td>Healthcare Provider</td>
<td>850</td>
<td>07/14/2016</td>
<td>Unauthorized Access/ Disclosure</td>
<td>Electronic Medical Record</td>
</tr>
<tr>
<td>North State University - MI College of Optometry</td>
<td>MI</td>
<td>Healthcare Provider</td>
<td>3947</td>
<td>10/11/2013</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>EnvisionRx</td>
<td>CH</td>
<td>Business Associate</td>
<td>540</td>
<td>10/31/2015</td>
<td>Unauthorized Access/ Disclosure</td>
<td>Network Server</td>
</tr>
<tr>
<td>Indiana University School of Optometry</td>
<td>IN</td>
<td>Healthcare Provider</td>
<td>757</td>
<td>10/21/2011</td>
<td>Theft</td>
<td>Network Server</td>
</tr>
<tr>
<td>Visionworks Inc.</td>
<td>TX</td>
<td>Health Plan</td>
<td>78884</td>
<td>11/10/2014</td>
<td>Loss</td>
<td>Network Server</td>
</tr>
<tr>
<td>REVE-WOODS EYE CENTER</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>30000</td>
<td>11/15/2014</td>
<td>Theft</td>
<td>Network Server</td>
</tr>
<tr>
<td>Visionworks Inc.</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>47663</td>
<td>11/21/2014</td>
<td>Theft</td>
<td>Network Server</td>
</tr>
<tr>
<td>Rabinsohn Eye Center PC</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>1749</td>
<td>12/20/2014</td>
<td>Theft</td>
<td>Desktop Computer</td>
</tr>
</tbody>
</table>

Are YOU HIPAA Compliant?

We are HIPAA compliant...
I had an expensive Security Risk Assessment done
Am I HIPAA compliant?
Policies & Procedures

- I have a Manual, I am compliant “right”?
Workforce Training

- I paid for my employees HIPAA training, I am compliant.

* Cost for 10 employee practice
Avoidable Breach

- **Who**: Anchorage Community Mental Health Services (ACMHS) - **Nonprofit org. (Alaska)**
- **What**: Malware caused breach of unsecured ePHI
- **Why**: “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 & CAP (Corrective Action Plan) (12/2014)
What is HIPAA Compliance and what is NOT

- **Compliance vs. Security**
  - Fines vs. Risk

- **HIPAA/HITECH**
  - Protect patient confidentiality while furthering innovation and patient care
  - Privacy Rule and Security Rule

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

- **Meaningful Use**
  - Accelerate adoption of EHR (electronic Health records)
Compliance vs. Security

Compliance:
- Audits
  - Security, Privacy, and Administrative
- Gap Identification
- Remediation
- Policies & Procedures
- Employee Training & Attestation
- Business Associate Management
  - BA Agreements & Audit
- Incident Management

Security:
- Security Risk Analysis
  - Penetration Testing
  - Vulnerability Scan
- Network Security
- Managed Services
- IT Consulting
- Cloud Services

Security Risk Assessment

FINES

RISK

REPUTATION

855-85-HIPAA
© 2017 Compliancy Group, LLC
Privacy Rule
Sets standards for when protected health information (PHI) may be used and disclosed.

Security Rule
Requires safeguards to ensure only those who should have access to electronic protected health information (ePHI) will have access.

Breach Notification Rule
Breaches of unsecured PHI require notifying HHS, affected individuals, and in some cases the media.

Security Audit
Privacy Audit
Administrative Audit

Meaningful Use
Risk Assessment
What Information Does HIPAA Protect?

PHI may include any of the following:

- Names
- Addresses
- Dates of Service
- Telephone Numbers
- Fax Numbers
- Email Addresses
- Social Security Numbers
- Medical Record Numbers
- Health Plan Beneficiary Numbers
- Account Numbers
- Certificate/License Numbers
- Vehicle identifiers/Serial Numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers;
- Biometric identifiers
- Full Face Photos or Videos
- Any other unique identifying number, characteristic, or code
Omnibus Rule

- **Business Associates:**
  - Direct liability by function
  - Directly liable for violations
  - Must be HIPAA Compliant (Security Rule)
    - Technical, Administrative, & Physical Safeguards

- **Covered Entities:**
  - Compliance with Privacy Rule
  - Must have BAAs (Business Associate Agreements)
  - Conduct **Due Diligence**
  - for the CE

- **Contracting with subcontractors**
  - BA liability flows to all subcontractors
The Need For BAAs

- **Who**: Raleigh Orthopaedic (North Carolina)
- **What/Why**: 17,300 patients affected
  - Handed over PHI 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.”

Why Should I Worry About HIPAA?

HIPAA is the Law

- Current market solutions often only address pieces of compliance
- Enforcement is on the rise ↑
  - Record fines levied: **400% increase**
    - $6.2 Million in 2015
    - $24 Million in 2016
    - $11.4 Million so far in 2017*
  - Three prison sentences
  - Medical license revoked
  - State Attorney General levying fines

HIPAA Enforcement

“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

- $24 Million in 2016 - 400% increase
- $11.4 Million so far in 2017

- Three Prison Sentences
- Medical License Revoked
- State Attorney General levying 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.
7. Responding promptly to detected offenses and undertaking corrective action.

*Source HHS & OIG
Random odds ....

- Winning Lotto: 1 in 175 Million
- Attacked by a shark: 1 in 11.5 Million
- Hit by Lightning: 1 in 960,000
- Hole in One: 1 in 12,500
- Random HIPAA Audit: 1 in 10,000
- Meaningful use Audit: 1 in 10
- Breach-Related Audit: 1 in ?
Causes Of A HIPAA Audit

- Phase 2 Random
- Meaningful Use Failure
- Business Associates
- Breach Notification

Audit Risk-O-Meter
- Low
- Medium
- High

Reported
- Whistleblower
- Complaint
The Process Of An Audit

Desk Audit
Request for Gap and Remediation Report

On Site Audit
Review of all 7 Elements of Effective Compliance

Results
Corrective Action Plan | Fines
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.**”

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.”
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."

But...It Probably Won’t Happen To Me

- In a recent study, more than half of business associates (59%) reported a data breach in the last two years that involved the loss or theft of patient data. More than a quarter (29%) experienced two breaches or more.
- Of the 345 incidents reported by HHS and listed on their site under Breaches Affecting 500 or More Individuals, 74 involved a business associate (21%).

Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data conducted by Ponemon Institute
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.”

Solving The HIPAA Compliance Puzzle

Audits
SRA (Security Risk Assessment), Administrative, Privacy

Remediation Plans

Incident Management & Remediation

Business Associate Management

Document Version, Employee Attestation & Tracking

Policies, Procedures & Training
We simplify compliance so you can confidently focus on your business.

Compliancy Group
855-85-HIPAA
855-854-4722
info@compliancygroup.com
www.CompliancyGroup.com

Marc Haskelson
President & CEO
855-854-4722 Ext 507
Marc@compliancygroup.com