HIPAA Audit – Don’t just “bet the odds”

“Good luck is a residue of preparation.” – Jack Youngblood

Braun Tacon – Process Architect / Auditor – Owner: www.MajorIncidentHandling.com
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 ?
HIPAA At A Glance

- **HIPAA – Aug 1996**
  - Provide for HCI portability between jobs while furthering innovation and patient care
  - Privacy Rule published Dec 2000 & Aug 2002
  - Security Rule published Feb 2003
  - Enforcement Rule final – Feb 2006

- **HITECH / Meaningful Use (MU) – Feb 2009**
  - Incentivize use of EMRS through cash payments
  - Added BA’s and Third Parties to the RACI list
  - Introduced the Breach Notification Rule

- **Omnibus – Jan 2013**
  - Dot the I’s, Cross the T’s, Tie it all together
  - Emphasis on increased enforcement / fines

- **Corrective Actions and / or Fines – Ongoing**
Enforcement Accelerating in 2016 and Beyond

Some 2016 Enforcement Examples

<table>
<thead>
<tr>
<th>Entity</th>
<th>Financial Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feinstein Institute for Medical Research</td>
<td>$3.9 Million</td>
</tr>
<tr>
<td>University of Mississippi Medical Center</td>
<td>$2.75 Million</td>
</tr>
<tr>
<td>Oregon Health &amp; Science University</td>
<td>$2.7 Million</td>
</tr>
<tr>
<td>New York Presbyterian</td>
<td>$2.2 Million</td>
</tr>
<tr>
<td>North Memorial Health Care</td>
<td>$1.55 Million</td>
</tr>
<tr>
<td>Raleigh Orthopaedic Clinic, P.A</td>
<td>$750,000</td>
</tr>
<tr>
<td>Catholic Health Care Services of the Archdiocese of Philadelphia</td>
<td>$650,000</td>
</tr>
<tr>
<td>Lincare, Inc.</td>
<td>$239,800</td>
</tr>
<tr>
<td>Complete P.T., Pool &amp; Land Physical Therapy</td>
<td>$25,000</td>
</tr>
</tbody>
</table>

- OCR has investigated and resolved over 24,617 cases by requiring changes in privacy practices and corrective actions.
- OCR has investigated complaints against many different types of entities including: national pharmacy chains, major medical centers, group health plans, hospital chains, skilled nursing facilities and small provider offices.
- Since OCR’s first resolution agreement in 2008, to date (November 2016), OCR has settled 41 such cases resulting in a total dollar amount of $48,679,700.00.

Source: U.S. Department of Health and Human Services

Source: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html
Threat Vectors For A HIPAA Audit

- Business Associates
- Phase 2 Random
- Meaningful Use Failure
- Breach Notification
- Reported *
  - Whistleblower
  - Complaint

* HHS is REQUIRED by law to investigate ALL HIPAA violation complaints
Phase 2 Random Audits

- Covered Entities and Business Associates will be randomly audited
- Began: March 22, 2016
- Business Associates sometime late 2016
- Will not end. Enforcement is accelerating
Meaningful Use Failure

- 5-10% of providers will be audited by CMS at random
- Having a Security Risk Assessment for Meaningful Use **does not** make you HIPAA Compliant
Complaint or Report Investigations

- Complaint of Security/Privacy violation
  - HHS is REQUIRED by law to investigate ALL HIPAA violation complaints

- Whistleblower
  - Frequently anonymous
  - Sometimes collect a percentage of any money collected
Breach Notification Required

Breach Notification Rule

- **Affects < 500 PHI**: must notify all breaches of calendar year by a deadline
- **Affects > 500 PHI**: must notify HHS immediately, publicized in HHS Wall of Shame

### Breach Report Results

<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>Florida Medical Clinic, PA</td>
<td>FL</td>
<td>Healthcare Provider</td>
<td>1000</td>
<td>05/04/2016</td>
<td>Unauthorized Access/Disclosure</td>
<td>Electronic Medical Record</td>
</tr>
<tr>
<td>Managed Health Services</td>
<td>IN</td>
<td>Health Plan</td>
<td>610</td>
<td>05/03/2016</td>
<td>Unauthorized Access/Disclosure</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Northstar Healthcare Acquisitions LLC</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>19988</td>
<td>04/20/2016</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Family &amp; Children’s Services of Mid Michigan, Inc.</td>
<td>MI</td>
<td>Healthcare Provider</td>
<td>981</td>
<td>04/27/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Children’s National Medical Center</td>
<td>DC</td>
<td>Healthcare Provider</td>
<td>4107</td>
<td>04/16/2016</td>
<td>Unauthorized Access/Disclosure</td>
<td>Network Server</td>
</tr>
<tr>
<td>Mayfield Clinic Inc</td>
<td>OH</td>
<td>Hospital</td>
<td>50000</td>
<td>04/22/2016</td>
<td>Unauthorized Access/Disclosure</td>
<td>Other</td>
</tr>
<tr>
<td>Ohio Department of Mental Health and Addictions Services</td>
<td>OH</td>
<td>Healthcare Provider</td>
<td>992</td>
<td>04/23/2016</td>
<td>Hacking/IT Incident</td>
<td>Email</td>
</tr>
<tr>
<td>Kaiser Foundation Health Plan, Inc.</td>
<td>CA</td>
<td>Business Associate</td>
<td>2451</td>
<td>04/22/2016</td>
<td>Theft</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Wyoming Medical Center</td>
<td>WY</td>
<td>Healthcare Provider</td>
<td>3184</td>
<td>04/20/2016</td>
<td>Hacking/IT Incident</td>
<td>Email</td>
</tr>
<tr>
<td>Lake Pulmonary Critical PA</td>
<td>FL</td>
<td>Healthcare Provider</td>
<td>648</td>
<td>04/20/2016</td>
<td>Theft</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Lake Pulmonary Critical Care PA</td>
<td>FL</td>
<td>Healthcare Provider</td>
<td>648</td>
<td>04/20/2016</td>
<td>Theft</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Quarles &amp; Brady, LLP</td>
<td>WI</td>
<td>Business Associate</td>
<td>1032</td>
<td>04/19/2016</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
</tbody>
</table>

![Audit Risk-O-Meter](image)
### Full Year Breach Statistics 2016 / 2015

#### Largest Healthcare Breaches of 2016

<table>
<thead>
<tr>
<th>Rank</th>
<th>Entity Type</th>
<th>Cause of Breach</th>
<th>Records Exposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Healthcare Provider</td>
<td>Hacking/IT Incident</td>
<td>3620000</td>
</tr>
<tr>
<td>2</td>
<td>Business Associate</td>
<td>Hacking/IT Incident</td>
<td>3466120</td>
</tr>
<tr>
<td>3</td>
<td>Healthcare Provider</td>
<td>Hacking/IT Incident</td>
<td>2213597</td>
</tr>
<tr>
<td>4</td>
<td>Healthcare Provider</td>
<td>Hacking/IT Incident</td>
<td>882590</td>
</tr>
<tr>
<td>5</td>
<td>Healthcare Provider</td>
<td>Hacking/IT Incident</td>
<td>749017</td>
</tr>
<tr>
<td>6</td>
<td>Healthcare Provider</td>
<td>Unauthorized Access/Disclosure</td>
<td>651971</td>
</tr>
<tr>
<td>7</td>
<td>Healthcare Provider</td>
<td>Hacking/IT Incident</td>
<td>531000</td>
</tr>
<tr>
<td>8</td>
<td>Healthcare Provider</td>
<td>Loss</td>
<td>483063</td>
</tr>
<tr>
<td>9</td>
<td>Healthcare Provider</td>
<td>Theft</td>
<td>400000</td>
</tr>
<tr>
<td>10</td>
<td>Health Plan</td>
<td>Hacking/IT Incident</td>
<td>381504</td>
</tr>
<tr>
<td>11</td>
<td>Healthcare Provider</td>
<td>Hacking/IT Incident</td>
<td>300000</td>
</tr>
<tr>
<td>12</td>
<td>Healthcare Provider</td>
<td>Theft</td>
<td>205748</td>
</tr>
<tr>
<td>13</td>
<td>Healthcare Provider</td>
<td>Unauthorized Access/Disclosure</td>
<td>201000</td>
</tr>
<tr>
<td>14</td>
<td>Healthcare Provider</td>
<td>Improper Disposal</td>
<td>113528</td>
</tr>
</tbody>
</table>

#### 2016 Healthcare Data Breaches of 500 or More Records

<table>
<thead>
<tr>
<th>Year</th>
<th># of Breaches (500+)</th>
<th># of of Records Exposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>324</td>
<td>16,586,112</td>
</tr>
<tr>
<td>2015</td>
<td>270</td>
<td>113,267,174</td>
</tr>
</tbody>
</table>

#### Breaches of More Than 500 Records

<table>
<thead>
<tr>
<th>Year</th>
<th>500 to 1000</th>
<th>1,000 to 10,000</th>
<th>10k to 100k</th>
<th>100,001+</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>88</td>
<td>157</td>
<td>64</td>
<td>14</td>
</tr>
<tr>
<td>2015</td>
<td>76</td>
<td>142</td>
<td>37</td>
<td>12</td>
</tr>
</tbody>
</table>

#### Main Cause of Breach

- **2015**: Unauthorized Access/Disclosure 102, Hacking/IT Incident 57, Theft 81, Loss 23, Improper Disposal 6

- **2015**: Majority of 500+ Breaches due to Device Theft
- **2016**: Majority of 500+ Breaches due to Hacking Etc.
- Hacking and the theft / loss of IT devices will continue to challenge providers who do not fully appreciate the huge risks of poorly secured IT Networks and unencrypted devices that are supporting EMRs & ePHI.

So I’m Getting Audited – What’s Next?

Business Associates

Phase 2 Random

Meaningful Use Failure

Breach Notification

Audit Risk-O-Meter

Reported *
- Whistleblower
- Complaint

* HHS is REQUIRED by law to investigate ALL HIPAA violation complaints

- Low
- Medium
- High
What to Expect if You Get Audited

Desk Audit

Request for Gap and Remediation Report

Which Could Lead to

On Site Audit

Review of all 7 Elements of Effective Compliance

Both Types Can Lead to Either:

Results

Corrective Action Plan | Fines

OR BOTH
Audit Outcome – Malware Infection (Hacking)

- **Who:** University of Massachusetts Amherst (UMass)
- **What:** A workstation was infected with malware (virus) that may have led to the release of the ePHI of over 1,670 individuals
- **Why:** A lack of appropriate policies and procedures, inappropriate or missing technical security measures, as well as the absence of comprehensive risk analysis all contributed to the OCR Audit and Fine
- **Settlement:** $650,000 and CAP (Corrective Action Plan) (11/6/16)

Source: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/umass
Audit Outcome – Laptop Loss / Theft

- **Who:** University of Mississippi Medical Center (UMMC)
- **What:** Laptop loss / theft, 10,000 patient records
- **Why:** A lack of appropriate policies and procedures, failure to implement physical safeguards, failure to assign unique user names and allowing shared access to ePHI all contributed to the OCR Audit and Fine
- **Settlement:** $2,750,000 and CAP (Corrective Action Plan) (7/7/2013)

Source: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/UMMC/index.html
All These Outcomes Sound Bad

• Yes, many of the potential outcomes are not good

• HHS is incented to enforce with prejudice, after an Inspector General (IG) Report called out the HHS for poor enforcement

• Expect more “Wall of Shame” type tactics as well as increasing financial penalties in the name of enforcement and PR

• Looks like the odds are against me. What can I do?
Your Best Defense Is A Good Offense

- Review your current HIPAA risk analysis procedures

- Review your policies and procedures to ensure compliance with all HIPAA Requirements, including those considered “addressable”, as well as the recent Breach Notification Rule

- Every portable devices (laptops/smartphone/med-device) that does or can contain PHI must be encrypted by Policy and must be verifiably enforced. Remote wipe is a big plus

- Don’t ignore new and significant threats. Do you know what “RansomWare” is? If you don’t, you need to find out ASAP
It All Begins With A Risk Analysis

<table>
<thead>
<tr>
<th>Implementation Specification</th>
<th>R/A</th>
<th>Threat Description</th>
<th>Risk Assessment Question</th>
<th>Risk</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Use the Threat / Risk Impact Matrix to the right to compute the Risk Score</td>
<td>Threat Likelihood</td>
<td>Risk Impact</td>
</tr>
</tbody>
</table>


Policies and procedures to prevent, detect, contain, correct security violations

Risk Analysis: Required

Conduct an accurate and thorough assessment

Unidentified / unknown vulnerabilities present increased risk to patient data and the systems that store and process it. Risks include any threat source that may impact the confidentiality, integrity, and/or availability of patient data.

Has a Risk Analysis been completed to identify potential threats & vulnerabilities and likelihood of impact, including management, operational, and technical issues (such as outlined in NIST SP 800-30), for all systems that create, receive, maintain, or transmit ePHI?
Have Questions?
Need Help?
Risk Analysis or Assessment?
Business Continuity or Disaster Planning?

info@MajorIncidentHandling.Com