HIPAA Compliance and Behavioral Health
Compliancy Group
We simplify compliance!

Started in 2005 by HIPAA auditors & Compliance experts
- Market need for a solution for the end-client
- Proprietary Achieve, Illustrate and Maintain methodology
- Confidently satisfy HIPAA, HITECH and Omnibus regulations

Compliance is our business
- No client has ever failed an OCR or CMS audit
- 100% of our clients would refer us to a friend
- Recognized Leader of Compliance
  - Top Compliance Tools & Emerging Vendor
  - Featured in multiple publications
- Endorsed by Industry Leaders and Associations

© 2007-2016
Are YOU HIPAA Compliant?

We are HIPAA compliant...
Risk Assessments

- I had an expensive Security Risk Assessment done
- Am I compliant now?
Policies and 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.
- **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)

Problems with Compliance Today

- 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
HIPAA Enforcement

Who is being fined?

- Settlements so far in 2016 have totaled **more than any year prior** $8,664,800

- **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

*As of May 2016*
What is HIPAA?

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

- **Omnibus**
  - Business Associates must protect PHI

- **Meaningful Use**
  - Accelerate adoption of EHR (electronic Health records)

- **Compliance vs. Security**
  - Fines vs. Risk
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.
HIPAA Security Rule Standards

Administrative Audit

Privacy Audit

Security Audit

Meaningful Use Risk Assessment
Security AND Privacy Rule

- **Who:** Insurance company, Triple-S (Puerto Rico)
- **What/Why:** Widespread non-compliance
  - Failure to implement **Administrative, Privacy, and Technical** safeguards
  - Lack of appropriate **Business Associate Agreements**
  - Failure to conduct **accurate/thorough Risk Analysis**
- **Settlement:** $3.5 Million & CAP (11/30/15)

“This case sends an important message for HIPAA 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**, including those addressing business associate agreements and the minimum necessary use of protected health information.”

- Jocelyn Samuels, Director of OCR

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**: $1,550,000 and CAP (3/19/16)

“Two major cornerstones of the HIPAA Rules were overlooked by this entity. 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.

- Jocelyn Samuels, Director of OCR

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
### 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>Ohio Department of Mental Health and Addiction Services</td>
<td>OH</td>
<td>Healthcare Provider</td>
<td>56000</td>
<td>04/22/2016</td>
<td>Unauthorized Access/Disclosure</td>
<td>Other</td>
</tr>
<tr>
<td>Woodhull Medical and Mental Health Center</td>
<td>NY</td>
<td>Healthcare Provider</td>
<td>1581</td>
<td>10/19/2015</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>New York State Office of Mental Health Nathan S. Kline</td>
<td>NY</td>
<td>Healthcare Provider</td>
<td>563</td>
<td>04/10/2015</td>
<td>Loss</td>
<td>Laptop</td>
</tr>
<tr>
<td>Institute for Psychiatric Research</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Region Six of the Georgia Dental Health and Developmental</td>
<td>GA</td>
<td>Healthcare Provider</td>
<td>3387</td>
<td>10/09/2014</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Disabilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Valley Mental Health</td>
<td>UT</td>
<td>Healthcare Provider</td>
<td>700</td>
<td>04/26/2013</td>
<td>Theft</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>Cuyahoga County Board of Developmental Disabilities</td>
<td>OH</td>
<td>Healthcare Provider</td>
<td>613</td>
<td>11/20/2012</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Hawaii State Department of Health, Adult Mental Health</td>
<td>HI</td>
<td>Healthcare Provider</td>
<td>674</td>
<td>11/20/2012</td>
<td>Hacking/IT Incident</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>Division</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Union County Board of Developmental Disabilities</td>
<td>OH</td>
<td>Health Plan</td>
<td></td>
<td>11/05/2012</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
</tbody>
</table>

<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 Psychotherapy, LLC</td>
<td>WI</td>
<td>Healthcare Provider</td>
<td>509</td>
<td>12/23/2015</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>New York State Office of Mental Health Nathan S. Kline Institute for Psychiatric Research</td>
<td>NY</td>
<td>Healthcare Provider</td>
<td>563</td>
<td>04/10/2015</td>
<td>Loss</td>
<td>Laptop</td>
</tr>
<tr>
<td>Multilingual Psychotherapy Centers, Inc</td>
<td>FL</td>
<td>Healthcare Provider</td>
<td>3600</td>
<td>10/28/2014</td>
<td>Theft</td>
<td>Network Server</td>
</tr>
<tr>
<td>Comprehensive Psychological Services LLC</td>
<td>SC</td>
<td>Healthcare Provider</td>
<td>3500</td>
<td>11/01/2013</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
</tbody>
</table>
The NEED For BAAs

- **Who**: Raleigh Orthopaedic (North Carolina)
- **What**: Breach report, 17,300 patient records
- **Why**: Handed over x-rays and associated PHI to potential business partner without first executing a business associate agreement.
- **Settlement**: $750,000 and 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. It is critical for entities to know to whom they are handing PHI and to obtain assurances that the information will be protected.”

- Jocelyn Samuels, Director of OCR

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
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

855-85-HIPAA
www.compliancygroup.com
Laptop Theft

- **Who:** A radiation oncology private physician practice, Cancer Care Group, P.C.
- **What:** A laptop theft lead to breach
- **Why:** But lack of comprehensive risk analysis and device and media control policy lead to a steep penalty
- **Settlement:** $775,000 and CAP (Corrective Action Plan) (9/2/15)

Mishandling PHI

- **Who:** Kokomo-area **dentist**, Dr. Joseph Beck
- **What/Why:** “Mishandled medical records containing sensitive information of more than 5,600 patients.”
  - **Improper disposal** of PHI records
- **Settlement:** $12,000 and Dr. Beck’s license to practice dentistry was **permanently revoked** (1/9/15)

Compliance Questions?

For more information, contact:

855-85-HIPAA
info@compliancygroup.com

Marc Haskelson
855-854-4722 ext 507
marc@compliancygroup.com