Assessing your HIPAA Risk And Breach Readiness
Objectives/Agenda

**What are the recent revisions to HIPAA**
- Explain the revised HIPAA Privacy Rule
- Explain recent OCR/HHS Activities
- How might this effect you?

**Definition of “breach” and clarity on PHI**
- What is a breach and what determines exposure?
- What is PHI?

**Components to a Creating a HIPAA Culture/Case Study**
- Creating a HIPAA compliant culture
  - Current State Analysis Approach and Description
- Remove any mystery or concerns related to the Risk Assessment
- Review some real project outcomes
  - Colorado Choice Health Plans
  - 150 Employee health plan in rural Colorado

**Who is Himes Consulting Group**
- Background experience and representative clients
The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law. This is the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009.
Update on HIPAA recent activities

Phase 2 of the OCR Audit Protocols were created to increase OCR’s oversight of Covered Entities and Business Associates.

- All covered entities and business associates not currently being investigated for a complaint or breach are subject to proactive selection for a compliance desk audit.

- Covered entities and business associates will have 10 business days to comply to the OCR Requests.

- The 2016 audit protocols provide more detail for guiding design and implementation of policies and procedures.

- The Phase 2 HIPAA Audit Program reviews the policies and procedures adopted and employed by covered entities and business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules.
How Big is the Business Issue?

PHI is being accessed at an alarming rate¹:

- Nearly 87% occur in the US
- 90% occur across just 20 industries
- 40% of breaches due to “insider” malicious acts and accidental breaches
- $19 million in fines issued in 2016³
- Breach incidents projected to increase 10% by year end 2016³
  - Veterans Administration experienced a 36% increase in Data Breaches in one month in 2015

Costs of Breach continue to grow²:

- Costs of data breaches have set a new record and are both:
  - Direct (35%) – Increased security, fines, recovery, restitution and;
  - Indirect (65%) – Brand recovery, public relations, lost revenue

---

1: VPH Data Breach report
2: Ponemon Institute report

Millions are spent on new technology along with countless hours to implement but we are as vulnerable as our most uninformed employee
How Big is the Business Issue?

Data Breach Facts

- Nearly 90% of health care organizations had a data breach in the past 2 years.
- Publically posted breaches (>500 records) represent less than 1% of all reported breaches (<500 records)
- Nearly 50% had more than 5 data breaches in the past 2 years.
- The average cost of a large, reportable data breach is estimated to be more than $4 million.

Top Five Root Causes of the Data Breaches:

Healthcare Organization/Business Associates
1. Criminal Attack
2. Issues with Third Party
3. Stolen Computing Device
4. Unintentional Employee Action
5. Technical Systems Glitch
What is a Breach and What Determines Exposure?

What is a Breach:

- “An impermissible use or disclosure of Protected Health Information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the Protected Health Information (PHI) has been compromised based on a risk assessment.

What determines whether PHI has been compromised:

- Likelihood of Re-identification

- Un-authorized person who has used or had the disclosure made to

- Whether the PHI was actually viewed

- The extent to which the PHI has been mitigated

Protecting PHI & PII is job number one for HIPAA Covered Entities and now for Business Associates under the Omnibus Ruling.
Liability under HIPAA Breach and Omnibus Ruling

Major efforts occurring in 2016 and 2017

• Proactive Desk Audits and Onsite Audits being conducted in 2016 and 2017
  • 300 Desk Audits of Covered Entities, 100 Desk Audits of Business Associates
• Onsite Audits being initiated in 2017

Covered entity now has direct liability responsibility for both their own agents as well as all their business associates

• CEs engaging in business transactions with Business Associates - who will encounter PHI in the course of the business transaction - must ensure that a Business Associate Agreement is in place before any PHI is provided or accessed by the Business Associate

• Any Covered Entity which does not implement the required controls now faces financial penalties, sanctions, and potential loss of license. Criminal proceedings can also be initiated for failing to secure PHI

Business Associate also is liable for acts of agents within scope of agency including agents who are subcontractor business associates
What is PHI?

PHI (Protected Health information) is a combination of personal identifiers linked together to become identifiable data. These personal identifiers include but are not limited to:

- Name
- Address
- Date of Birth
- Admission Date
- Date of Death
- Telephone & Fax numbers
- Email Address
- Medical Record #
- Health Plan Beneficiary #
- Social Security #
- Driver License #
- User ID & Passwords
- Account Number
- Certificate /license number
- Vehicle or other device number
- Web URL
- Internet Protocol IP address
- Finger or voice prints
- Photographic images
- Medical History or Treatment
- Financial Information
- Credit Cards
- Insurance
- Bank Account numbers
- Office Location
- Badge Number
- Biometrics
- Legal Information
- Military Information

Sources: [http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html](http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html) and other industry sources.
What is Involved in Creating a HIPAA Culture

HIPAA Awareness/Training and a Current State Risk Analysis are the minimum threshold that OCR and HHS are looking for to show active participation from Covered Entities.
What are the Financial Impacts?

2016 Notable Breaches

• **Advocate Healthcare- $5.5 Million.** OCR stated that they *failed to conduct an appropriate risk analysis*, limit physical access to their large data center, to obtain BAAs and to safeguard unencrypted laptop PCs. These widespread allegations and non-compliance have occurred for more than a decade.

• **University of Mississippi Medical Center- $2.75 Million.** A breach report for a stolen laptop from the ICU that did not have the proper security installed. OCR determined that UMMC was aware of risks and vulnerabilities since April 2005, yet failed to implement corrections.

• **Oregon Health & Science University (OHS), $2.7 Million.** A breach report regarding unencrypted laptops and an unencrypted thumb drive. The OCR determined the *risk analysis completed by OHS were not comprehensive* and the OCR found evidence of widespread unmitigated vulnerabilities.
What are the Financial Impacts?

2016 Notable Breaches continued

• **Northwell Health- $3.9 Million.** A breach report regarding the theft of a laptop computer with over 13,000 patient and research participants on it. The OCR determined that Feinstein’s security management process was deficient.

• **Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS)- $650,000.** The theft of a single unencrypted iPhone with information on 412 individuals. OCR discovered CHCS had *no risk analysis*, no risk management plan, and no policies regarding removing mobile devices from its facility and no security incident procedure.
How Can My Organization Prepare?

5 Key Attributes of Achieving Safeguard Compliance

• Conducting a Written Risk Analysis – Reviewing and updating periodically

• Implementing Safeguard Policies and Procedures – Compliant with standards and tailored to findings from Risk Analysis – Accessible to all workforce members

• Maintaining Written Documentation of Safeguard Actions – Written (can be electronic) and retained for 6 years from last action

• Designating Privacy and Security Officials – Can be same individual

• Training of Workforce Members on Safeguard Policies and Procedures – Awareness and understanding of safeguards, with sanctions for violations
Current State Analysis Approach

To create a cultural change, the Current State Analysis needs to be reviewed from three unique, but complimentary perspectives:

**Cultural Impact**
- How an organization approaches PHI and compliance
- How that approach weaves compliance into the fabric of day-to-day operations

**Risk Assessment**
- Identifying, Evaluating and Prioritizing risks
  Based on specific OCR and DHS policies and procedures.

**Process Impact**
- Identify how compliance applies to process groups
- Align Risks to Functions to ease with targeted fixes
Current State Analysis Project Description

Case Study

Project Scope

- Conduct a current state assessment of the potential HIPAA Risks across the organization with an emphasis on business operations vs. technical or cyber exposure.

Resource Needs

- HCG: Team of 3 - 4
- CO Choice: Access to Senior Management and key individuals of each function.

Timeline

Project Duration: 3 Weeks

Key Project Deliverables

- Graphical representation of risk areas across the existing process flows
- Detailed Risk Analysis aligned with HHS and Office of Civil Rights requirements
- Documented Action Plan for recommendations or remediation

HIPAA Privacy focus

- Effort was focused on the business operations, including technology.
Colorado Choice Perspective

Project Objectives
The most important part of an effort like this was to understand what it would take to create a culture of compliance that:

- Becomes 2nd nature to the employees affected
- Becomes “who you are” as an organization
- Is so engrained into the culture that it is not an afterthought, it is woven into the fabric of the organization

Privacy Consideration for Rural

- In a large company, sense of anonymity may exist because the potential of an employee personally knowing the customers that they may be processing is small
- In rural organizations, there is little anonymity and its quite possible and in some cases likely that employees may be processing transactions of neighbors, family or friends
- An understanding of what the boundaries are for privacy is more critical in the rural market than perhaps the urban environment
Colorado Choice Perspective

Key Learnings

- There was an understanding of the need for Cultural change, not just annual HIPAA privacy awareness assessment

- Initially felt that the approach was going to be “too comprehensive”
  - Basing that on previous work with the NIST technology assessment that was completed as part of the URAC accreditation

- Outcome was:
  - Comprehensive
  - In-depth

- Level of effort was required to uncover the cultural risk areas in each of the processes to offer a tangible action plan to execute

- Independent GAP Assessment provides
  - An objective perspective that is fact-based, not personality-based or historically-based which may occur if performed internally
  - A Roadmap for implementation which then can be prioritized and budgeted internally for sequencing and implementation execution
HIPAA Applies Across All Key Departments

HIPAA applies to all departments within a Hospital and HCG subscribes to a methodology that applies the Culture of Compliance at the functional level to ensure that it gets incorporated into all activities. Below are a list of candidate Clinical and Non-Clinical departments and functions that could be included in this evaluation:

**Clinical Departments**
- Allergy and Immunology
- Behavioral Health
- Cardiology
- Dentistry
- Dermatology
- Endocrinology
- Family Practice
- Gastroenterology
- General Medicine
- General Surgery
- Gynecology
- Hematology
- Intensive Care
- Internal Medicine
- Neonatology
- Nephrology
- Neurology
- Nursing Services
- Obstetrics
- Occupational Therapy
- Oncology
- Ophthalmology
- Optometry
- Otorhinolaryngology
- Orthopedics
- Pain Management
- Pediatrics
- Physical Therapy
- Psychiatry
- Pulmonary
- Urology
HIPAA Applies Across All Key Departments

<table>
<thead>
<tr>
<th>Non Clinical Departments</th>
<th>Supporting Services</th>
<th>Ancillary Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ambulance Services</td>
<td>Legal and Audit</td>
<td>Electrical</td>
</tr>
<tr>
<td>Anesthesiology</td>
<td>Materials Management</td>
<td>Facilities Management</td>
</tr>
<tr>
<td>Billing</td>
<td>Medical Records</td>
<td>– Engineering</td>
</tr>
<tr>
<td>Blood Bank</td>
<td>Pathology</td>
<td>– Transportation</td>
</tr>
<tr>
<td>Case Management</td>
<td>Pharmacy</td>
<td>Housekeeping</td>
</tr>
<tr>
<td>Central Sterile Services Department</td>
<td>Oncology</td>
<td>Laundry Services</td>
</tr>
<tr>
<td>Collections</td>
<td>Admitted</td>
<td>Security</td>
</tr>
<tr>
<td>Communications</td>
<td>Non Admitted</td>
<td>Security Obstetrics</td>
</tr>
<tr>
<td>Compliance</td>
<td>Public Relations</td>
<td></td>
</tr>
<tr>
<td>Customer Service</td>
<td>Quality</td>
<td></td>
</tr>
<tr>
<td>Development</td>
<td>Radiology</td>
<td></td>
</tr>
<tr>
<td>Dietary</td>
<td>– Nuclear Medicine</td>
<td></td>
</tr>
<tr>
<td>Food Services</td>
<td>– Ultrasound</td>
<td></td>
</tr>
<tr>
<td>Human Resources</td>
<td>Reception</td>
<td></td>
</tr>
<tr>
<td>Information Technology</td>
<td>Residency Program</td>
<td></td>
</tr>
<tr>
<td>Initial Operations</td>
<td>Scheduling</td>
<td></td>
</tr>
<tr>
<td>In Service Clinical Training</td>
<td>Social Work</td>
<td></td>
</tr>
<tr>
<td>Laboratory Services</td>
<td>Utilization Review</td>
<td></td>
</tr>
</tbody>
</table>
Himes Consulting Group is a Business Optimization company focused on improving an organization’s core processing efficiencies.

- Primary focus is on knowledge worker productivity ensuring they are equipped to work efficiently
- Over 25 years of experience helping large, medium-sized, and smaller organizations achieve and exceed their goals
- Provide consulting services to deliver measurable benefits, utilizing Senior Level talent to accelerate results

Results come from the relentless execution of core *blocking and tackling* activities
Why Himes Consulting Group?

Compliance and Regulatory

• Collectively, over 50 years of Provider and Payer experience
• Extensive understanding of workflow and process integration points across the Healthcare Value Chain
• Demonstrated experience working within Healthcare B2B business model in both for profit and not-for-profit environments
• Specific focus on creating a compliant Culture along with the processes and the infrastructure to support it
• Long track record of HIPAA-related and regulatory compliance work for over a decade
  ■ Working in HIPAA related process and compliance work since 2003
  ■ HCG team members are Certified HIPAA experts
  ■ Familiarity with Medicare/Medicaid having been the interim operations manager for a Med Advantage processing unit for a large, east-coast Blue Payor
  ■ Individuals with specific Provider and Provider-audit capabilities on each team to accelerate the results
Representative Clients
Questions?

For additional information, please contact:

**Rob Himes**  
Managing Partner  
Himes Consulting Group  
312-961-6656  
robhimes@himesconsulting.com

**Barbara Johnson**  
Senior Business Development Resource  
Himes Consulting Group  
773-817-0949  
barbarajohnson@himesconsulting.com