Audit and Compliance Realism: What Do I Really Need to Do to Be Secure

October 25, 2012
Industry leading Education

- Audit Realism: Effective Compliance and Protection Readiness
- HITECH/HIPAA: Understanding the Public Policy Rationale
- HIPAA Compliance Simplified: Demonstration of The Guard

Certified Partner Program

Certified Partners
Get the added confidence working with The Guard network, along with special programs for Guard users only

Why use our partners?
- Certified
- Approved Services
- Integrated with The Guard
- Special Pricing

Todays Webinar

- Please ask questions
- Todays slides are available
  http://compliancy-group.com/slides023/
- Past webinars and recordings
  http://compliancy-group.com/webinar/

855.85HIPAA
www.compliancygroup.com
Moderator
- Robert Zimmerman
  - IT Development, Audit and Compliance, Deloitte Risk Management Leader

Panelist
- Ty Faulkner
  Healthcare Education and Credentialing, ONC and HIMA HIT Instructor
- Susan Pretnar
  Health IT and Provider Relations, Blue Cross IT and Provider Support
1. Current State of Security and Privacy
2. What are the Greatest Risks
3. What do I Really Need to Do
4. Audit Readiness
5. Audit Process
6. Obtaining and Maintaining Compliance
7. Wrapup
The Yin and Yang of Security

Can we Implement Better Security, Enhance Privacy and Improve Productivity? YES!

- Minimize the productivity impact of security by making it as transparent as possible
- While security controls stop people from doing bad things, these same controls can enforce best practice
- There is great potential in using data on what people are doing to improve productivity
Data Breaches are More Prevalent than You think

* 2012 HIMSS Analytics Report
  * 31% of respondents said they had a data breach
  * 69% reported experiencing more than one breach

* What are likely factors for a Breach?
  * Lack of staff attention
  * Mobile Devices storing PHI
  * Health Information Sharing

* What’s the Cost of a Breach?
  * 81% resulted in time and productivity loss
  * 78% diminished brand or reputation
  * 75% loss of patient goodwill
Common ways a data breach can occur:

- Backing up PHI and taking it home
- Office mail containing PHI
- Employees being uneducated about the proper ways to store and discard private information
- Having unsupervised staff (i.e. cleaning crew or maintenance) working after hours
- Employees sharing stories about patient cases

Source: HHS Office of Civil Rights Report to Congress
Phoenix Cardiac Surgery agreed to pay HHS $100,000 and take corrective actions to protect patient information.

Complaint that the practice "was posting clinical and surgical appointments for its patients on an Internet-based calendar that was publicly accessible,“ The civil rights office's investigation also found that the practice "had implemented few policies and procedures to comply with the HIPAA privacy and security rules and had limited safeguards in place to protect patients' electronic protected health information."

OCR Director Leon Rodriguez said in the statement. "We hope that healthcare providers pay careful attention to this resolution agreement and understand that the HIPAA privacy and security rules have been in place for many years, and OCR expects full compliance no matter the size of a covered entity."
A dentist contacted our office indicating that a hygienist disclosed the name and information of patient in need of periodontal services to a hygiene student without permission. On being contacted by the student who offered to treat the patient at the hygiene school, the patient contacted the dentist to file a complaint for breaching his privacy. The dentist dismissed the hygienist.
The FBI arrested a former employee of Florida Hospital Celebration Health for accessing patients' emergency department records and selling them to a solicitor for attorneys and chiropractors, WFTV reports (WFTV, 8/17).

Dale Munroe accessed the files of patients who were treated for injuries resulting from automobile accidents at multiple hospitals across the state.

According to the complaint in U.S.A. v. Munroe, Munroe accessed about 763,000 patient records from late 2009 through mid-2011.

Munroe and his wife allegedly were paid approximately $10,000 for information from the records.

The hospital then:

- Fired Munroe, wife, and the other hospital workers involved
- Audited access to relevant records
- Launched a more extensive audit of access to ED patient data
It’s Easy to Sell Data on the Black Market

Amazingly Easy

- While sale of information takes place in underground forums, it is surprisingly easy to join
- Experts say PII of over 40 Million Americans is being bought and sold online
- Competing prices, additional services, money back guarantees
- Like any commodity market data is priced by value; does it belong to a real person, is it in demand, how commercial is it
As One Famous Hacker said…”The weakest link in any network is its people”

We can Blame Hackers. But just as there will always be software vulnerabilities there will always be hackers. The real question is how do we stop them.

So What Can We Do to Simply, Effectively, and Efficiently Protect our Organization’s PHI?
Where are You in the Risk Management Lifecycle

**Control Activities**
- Administrative
- Operational
- Technical

**Program**
- Policies
- Procedures
- Plans
- Assignments
- Schedules

**Domains**
- People
- Processes
- Technology

**Data Protection**
- Risk Assessment
- Risk Management
- Risk Mitigation
- Monitoring, Analysis
- Documentation

**Compliancy Group**

**HIPAA HITECH EXPRESS**
What do I Really Need to Do?

- Risk Analysis
- Prioritized Requirements Gap Analysis
- Mitigation Workplan and Strategy
- Remediate Critical Risks and implement Mitigating Controls
- Core Policies and Procedures
- Plans
  - Risk Management
  - Incident Response
  - Contingency /Business Continuity
  - Physical Security

*Maintain evidence that Security & Privacy processes and controls are in place and working*
Compliance Audits, Yesterday and Today

Traditional
- Review and assess all requirements and controls
- Act like an Auditor
- Treat everything in Black and White
- Focus on what’s wrong; what audit points can we identify

Risk Based
- Focus on High Priority and Critical risks and requirements
- Act like an Advisor
- Give Credit for Effort and Intent
- Focus on Remediation and providing Guidance

HIPAA HITECH EXPRESS
**Risk Based Approach is More Effective**

- Focus resources on what is important
- Focus on behavior, not just technology
- Integrate training into the mitigation process
- Utilize an iterative process that builds risk management capabilities
- Avoid negligence penalties
- Reduce costs
# Table 1: Categories of Violations and Respective Penalty Amounts Available

<table>
<thead>
<tr>
<th>Violation category—Section 1176(a)(1)</th>
<th>Each violation</th>
<th>All such violations of an identical provision in a calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A) Did Not Know</td>
<td>$100–$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(B) Reasonable Cause</td>
<td>1,000–50,000</td>
<td>1,500,000</td>
</tr>
<tr>
<td>(C)(i) Willful Neglect—Corrected</td>
<td>10,000–50,000</td>
<td>1,500,000</td>
</tr>
<tr>
<td>(C)(ii) Willful Neglect—Not Corrected</td>
<td>50,000</td>
<td>1,500,000</td>
</tr>
</tbody>
</table>
Auditors look for Consistency; Consistency and Standardization Reduces Risk

- Standard process is Repeatable and Drives Risk Management across Organizations and Exchanges
- Standardization is also Cost Effective
What do Auditors Look For

* Control Design Effectiveness
  * That required process and control is in place
  * Access Control Policies and processes have been developed

* Control Operating Effectiveness
  * That required process and control is actually working, being used
  * Access Controls are actually preventing unauthorized access and being monitored
Why Bother?

- If you Fit the Risk Profile You’re likely to be Audited
- You could be Chosen based on Geography and Size
- Effective security and privacy programs are driven by understanding of importance of mitigating
  - Reputational Risk
  - Revenue Risk
  - Operational Risk
- An important Result and Benefit is you reduce
  - Audit and Compliance Risk
Making Audits Successful for You

- Set a Point of Contact
- Ask for a List of Required Information
- Have Documentation Ready and Available
- Response to Data Requests Promptly
- Ensure Expectations and Timelines are Agreed To
- Let Other Team Members Know they May be Required
Audit Protocol

Initial 20 audits completed; additional 95 initial phase audits ongoing

The audit protocol was broken into three “modules” – privacy, security and breach notification.

Audit Protocol covers 81 Privacy control areas, 78 Security and 10 Breach Notification

* Privacy Rule Requirements
  * Notice of privacy, Rights to request privacy protection, Access of individuals, Administrative Requirements, Use and disclosure and Accounting of PHI
* Security Rule
  * Administrative, Physical and Technical safeguards
* Breach Notification Rule

Audit Protocol and Focus evolving; Standard process being developed.
HITECH Act requires periodic audits

Two Audit Contracts

* Booze Allen
  * Identify Audit Candidates
  * Provide background and recommendations for audit program

* KPMG
  * Develop audit protocol
  * Conduct pilot audit program
Any provider attesting to receive an EHR incentive payment for either the Medicare EHR Incentive Program or the Medicaid EHR Incentive Program should retain ALL relevant supporting documentation.

Documentation to support the attestation should be retained for six years post-attestation.

CMS, and its contractors (Figliozzi) will perform audits on Medicare and dually-eligible (Medicare and Medicaid) providers.

States, and their contractors, will perform audits on Medicaid providers.
What are Initial Round of Audits
Finding

Culture of Security and Privacy Understanding and Compliance is Evolving
* Incomplete Risk Analysis
* Undocumented Movement and Flow of PHI Data
* Missing or Out-of-Date Policies and Procedures
* Limited Security Awareness Training
* Disaster Recovery Plans not Tested
* Incident Response Process is Ad-hoc
* Limited Encryption
* Access Controls not Monitored
Attestation Process Will Get More Difficult

* Could easily have Providers in the same organization in different stages of Meaningful Use compliance in 2014
  * If 1st Year Provider follow Stage 1
  * If existing Provider than cover by Stage 2
What Can We Do To Secure De-Identified Data

- Prohibit the re-identification of individuals and their relatives, family or household members
- Require parties who wish to link new data elements with de-identified data to confirm that data remains de-identified
- Formally specifying that data recipients comply with specified time limits, data use restrictions, qualifications or conditions set forth
- Require those holding and using de-identified data to implement and maintain appropriate data security and privacy policies
- Require those who transfer de-identified data to third parties to enter into data use agreements
ProActive Risk Management Saves Time and Money

- On-going Monitoring and HIPAA HITECH compliance integration with other Governance, Risk and Control (GRC) initiatives
- Focus on exception reporting on incidence, security protection and access monitoring
- Include all Third Parties in Assessments
- Utilize a Prioritized Approach to see quicker results
- Engage the organization
Balancing Security, Compliance and Productivity

- Set security as an organization goal
- Utilize Training so everyone knows the basic rules
- Ensure management understands the risks associated with unsecured systems
- Communicate to the organization clearly
- Make sure everyone knows their roles and responsibilities
Process generates evidence required to manage and audit. No fire drills.
ONC’s advice to Healthcare Providers to Increase PHI Security

Leon Rodriquez recently appointed Director of HHS’s OCR said...

* Check that risk assessments are up to date
* Make sure senior managers are supportive of risk mitigation strategies
* Review existing compliance programs and staff training
* Ensure vigilant implementation of security and privacy procedures
* Conduct regular internal compliance audits
* Develop a plan for prompt response to breach incidents
The HIPAA HITECH EXPRESS SaaS based solution guides you through the compliance process and more, saving time, money and reducing risk.

- **Rapid Risk Assessment**
  Complete, Simple, Practical
  Guided, prioritized questionnaire that identifies critical risks and gaps

- **Rapid Remediation**
  Guided, Standard, Auditable
  Automated workflow and policy library to quickly and completely remediate risks and gaps

- **On-Going Monitoring**
  Repeatable, Documented, Compliant
  Effectively and efficiently manage the compliance, audit and incident response process

- **Integrated Training**
  Documented, Educational, Standard
  Train as you do
For more information on HIPAA HITECH EXPRESS, please contact:

**Robert Zimmerman**
robert.zimmerman@qipsolutions.com
Managing Director, Assurance Services
301-802-1925

**Eric Hummel**
Eric.hummel@qipsolutions.com
Managing Director, Security Services
703-980-3378
Compliance Simplified – Achieve, Illustrate, Maintain

Compliance Simplified!

✓ HIPAA Compliance
✓ HITECH Attestation
✓ Meaningful Use core measure 15

Free Demo and 15 Day Evaluation
855.85HIPAA
http://compliancy-group.com/

New & Past Webinars
http://compliancy-group.com/webinar/