A SIMPLIFIED BLUEPRINT FOR END TO END HEALTH IT RISK MANAGEMENT

Security & Privacy Compliance Readiness

HIPAA HITECH Express
Blueprint for Compliance Readiness

The Compliancy Group
Todays Speakers

- **Eric Hummel** has experience in IT and Security dating back more than 40 years. Eric has provided compliance oversight and security subject matter expertise to CISOs of 3 major Federal agencies, most recently the Department of Health and Human Services. As CEO of QI Partners, he is the principal architect and co-founder of the HIPAA HITECH Express and has developed the IT Security Process Library, one of its core elements.

- **Susan Pretnar** is currently President of KeySys Health, LLC, a woman owned healthcare consulting and technology company based in Birmingham, Alabama. She has more than 30 years experience in IT, Health Information Exchange development and implementation, Medicare operations management and various project management opportunities provided the expertise needed to develop and deliver solutions focused on major healthcare challenges; achieving Meaningful Use, and compliance with the HIPAA Security Rule.

- **Robert Zimmerman** has over 25 years of experience in financial and technology risk management in the public and commercial sectors. Robert has developed multiple successful risk management services including: Project Risk Management; PCI and FISMA compliance; and most recently Cloud Governance and HIPAA/HITECH Security and Privacy. As co-founder of the HIPAA HITECH Express his focus is on developing innovative and efficient approaches to mitigating and preventing the myriad of risks from the growth of Health IT.
AGENDA

• What’s the Security Privacy Value Proposition
• Reaching Your Goal: Protecting PHI
• Simplified Approach to Security Privacy Readiness
• Some Lessons Learned and Best Practices
• Open Forum
Data Breaches are More Prevalent than You think

- 2012 HIMSS Analytics Report
  - 27% of respondents said they had a data breach
  - 69% reported experiencing more than one breach
  - 79% said breach caused by employee

- 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
Data Breaches are Costly

- 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," according to an HHS news release. 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."
How Do We Value PHI?

- More healthcare organizations would invest in security if..
  - Understood privacy expectations of their patients
  - Understood increasing costs of class action law suits
  - Understood statistical probability of a data breach
- PHI Value Estimator free from ANSI
  - Estimates a potential cost of a data breach to an organization
  - Provides a methodology for determining an appropriate investment to reduce probability of a breach
  - Conduct Risk Assessment
    - Determine Security Readiness
      - Assess the Relevance of a Cost
      - Determine the Impact
    - Calculate the Total Cost of a Breach
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
- Medical data is worth 5 times the value of a Social Security #
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?
Simply, Effectively, and Efficiently Protect PHI
Reaching Our Goals: Walking Backwards

• Organization Goals
  • Be secure, stay secure
  • Be compliant, stay secure
  • No breaches
  • Spend next to nothing

• The best way to move toward all of these is to implement a Risk Management Program

• To do this we might:
  1. Hire a consultant to design and build a custom RM program
  2. Implement pre-existing security Risk Management solution and develop in-house capability for security management
  3. Implement pieces of the security program ad-hoc
  4. Cross our fingers
Risk Management Program

Program
- Policies
- Procedures
- Plans
- Assignments
- Schedules

Control Activities
- Administrative
- Operational
- Technical

Domains
- People
- Processes
- Technology
• Rapid Risk Analysis builds prioritized workplan
• Inventory of the enterprise
• Complete policy templates
• Standardized procedures implement the policies
• Reporting and Dashboards
• Outcome is Risk Management
Common Pitfalls to Avoid

- Reactive solutions
- Half solutions
- Point solutions
- Point-in-time solutions
- Lack of strategic goals and objectives
- Improper use of expertise
- Failure to implement review and verification
Simplified Approach, Rapid Results
Do You Have Basic Security in Place?

- Website of Gawker was hacked in 2011
- Turned Out over 3,000 Gawker users had the Password 123456
- Over 2,000 used password as the Password
- Simple Password Requirements could have prevented this

- Access Security Can Go a Long Way in Securing the Organization
A Simplified Approach to Security Privacy Compliance

- **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
## Simplified Risk Analysis Drives Remediation and Compliance Activities

<table>
<thead>
<tr>
<th></th>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Does your organization have the following documentation?</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td>Security Policies</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td>Security Procedures (e.g. Implementation of policies)</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>2</td>
<td>Does your organization have an inventory of all systems and applications that collect, process, store or transmit ePHI?</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>3</td>
<td>Is all ePHI present on workstations &amp; mobile devices encrypted?</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>4</td>
<td>Do all employees and temporary users of PHI undergo security training at least annually?</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>
Mitigation Map Drives Remediation and Ongoing Compliance

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA Citation</td>
</tr>
<tr>
<td>HIPAA Reference</td>
</tr>
<tr>
<td>Gap</td>
</tr>
</tbody>
</table>
| Mitigation Recommendation | • Define a set of roles for staff to be assigned  
• Assign each user to one or more roles  
• Train administrative staff in role and access management |
| Workflow Type | System Access Policies and Procedures Training |
| Audit Evidence Required | • Access Controls Policy  
• Security Awareness Training Curriculum  
• Logs of Access and Training attendance |
End to End Security & Privacy: Compliant, Secure, Auditable

Process generates evidence required to manage and audit. No fire drills.
ONC’s advice to Healthcare Providers to Increase PHI Security

Leon Rodriguez 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 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
Lessons Learned, Best Practices
Drive Effective Security
Unaware - Uninformed

• $ Spent on Security
  - Too small to quantify
• Employees not Technology
  - Both accidental and deliberate actors in breach incidents
• Everyday Security Needed
  - Develop a ‘culture’ of security awareness
• Patient & Provider Expectations
  - Greater access to personal health info, but protected
Security Best Practices High Tech + Low Tech

• Policies and Procedures – beyond defined
  - Implemented and monitored for effectiveness

• BAs and SLAs – Understand the ‘Chain of Trust’
  - Define accountabilities and responsibilities for mutual processes

• Breach Recovery – Logs, Logs, Logs
  - Why & how did it happen, who was affected – know where to look to protect your brand

• Invest in Technology
  - Cloud solutions expanding rapidly
  - Mobile devices greatly expand possibilities – safeguards are available

• Engage and Empower Patients – benefits of eHealth for all

• Risk Management Program – not a one time event
  - Ongoing business function needing time & $$
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
The Risk Averted

“Things alter for the worse spontaneously, if they be not altered for the better designedly”

Francis Bacon
British author and Statesman
QUESTIONS
The HIPAA HITECH Express Team can assist you reduce the complexity, confusion and guesswork of meeting the HIPAA security and privacy rules. Our solution walks you through the security and privacy compliance process, saving time, money and reducing risk. The HIPAA HITECH Express Team has done it before. We have extensive experience implementing risk based cost effective regulatory compliance and information security and privacy solutions.

For more information on HIPAA/HITECH Express contact:

Robert Zimmerman
rzimmerman@inforistec.com
301-802-1925

Eric Hummel
eric.hummel@qedsec.com
703-980-3378