Cal Slemp  
Managing Director, New York

Sensitive Data Management: Current Trends in HIPAA and HITRUST

Provide:

- An overview of key risks to healthcare organizations related to their handling of sensitive data.
- A discussion of the root causes of those risks and insight in possible mitigation techniques – especially in context to HIPAA and other data-related regulations.

- Protiviti’s Global Leader Security and Privacy Solutions
- Associated with IBM for 30 years prior to joining Protiviti, led their global Security and Privacy Services team
- Developed a unique identity management service offering for IBM called Trusted Identity
Agenda

• The Changing Landscape
• Causes For The Increased Sensitivity
• Additional Forces To Focus On
• Ideas For Efficiently Defining Your Risks and Addressing Them
• Summary and Discussion
The Changing Landscape
The Impact of OCR’s Ownership

<table>
<thead>
<tr>
<th>Year</th>
<th>Corrective Action</th>
<th>Investigated No Violation</th>
<th>Closed w/o Investigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Types of Violations (thru YE 2010)

<table>
<thead>
<tr>
<th>Standard or Specification</th>
<th>Type of Safeguard</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response and Reporting (R) 164.308(a)(6)(ii)</td>
<td>Administrative</td>
<td>179</td>
</tr>
<tr>
<td>Awareness &amp; Training 164.308(a)(5)(i)</td>
<td>Administrative</td>
<td>144</td>
</tr>
<tr>
<td>Access Control 164.312(a)(1)</td>
<td>Technical</td>
<td>141</td>
</tr>
<tr>
<td>Information Access Management 164.308(a)(4)(i)</td>
<td>Administrative</td>
<td>126</td>
</tr>
<tr>
<td>Workstation Security 164.310(c)</td>
<td>Physical</td>
<td>84</td>
</tr>
</tbody>
</table>
HHS Cops: Enforcement of Security Rule Poor

May 16, 2011

<table>
<thead>
<tr>
<th>SECURITY RULE VULNERABILITIES</th>
<th>HIGH IMPACT</th>
<th>MEDIUM IMPACT</th>
<th>LOW IMPACT</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Findings</td>
<td>Hospitals Affected</td>
<td>Findings</td>
<td>Hospitals Affected</td>
</tr>
<tr>
<td>TECHNICAL VULNERABILITIES</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Access</td>
<td>15</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control</td>
<td>38</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Control</td>
<td>9</td>
<td>5</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Integrity Control</td>
<td>21</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Person or Entity Authentication</td>
<td>9</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Transmission Security</td>
<td>14</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>TOTAL TECHNICAL</td>
<td>106</td>
<td>3</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>PHYSICAL VULNERABILITIES</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facility Access Control</td>
<td>2</td>
<td>1</td>
<td>10</td>
<td>3</td>
</tr>
<tr>
<td>Device and Media Control</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>TOTAL PHYSICAL</td>
<td>7</td>
<td>12</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>ADMINISTRATIVE VULNERABILITIES</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Management Process</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Workforce Security</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Incident Procedures</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contingency Plan</td>
<td>6</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Business Associate Contracts</td>
<td>6</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL ADMINISTRATIVE</td>
<td>11</td>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL VULNERABILITIES</td>
<td>124</td>
<td>24</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>
HITECH Violations Types (500+ thru 4/11)

- Theft: 50%
- Unauthorized Access/Disclosure: 18%
- Loss: 17%
- Improper Disposal: 5%
- Hacking/IT Incident: 7%
- Other: 1%
HITECH Violations Sources (500+ thru 4/11)

- Desktop Computer: 14%
- Laptop: 24%
- Paper Records: 23%
- Portable Electronic Device: 15%
- Network Server: 12%
- EMR: 3%
- E-mail: 3%
- Other: 6%
# Civil Monetary Penalty

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
<th>All Identical Violations per Calendar Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect-corrected in 30 days</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect-not corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

*OCR*
Causes For Increased Sensitivity
Utah's Medicaid Data Breach Worse Than Expected

Utah Department of Technology Services (DTS) reveals 780,000 individuals have been affected by the theft of sensitive Medicaid information. That's far worse than initial estimates.

By Nicole Lewis — InformationWeek
April 11, 2012 11:38 AM

CA Health Records Breaches Net $800,000 in Fines
November 22, 2010

Health Net discloses loss of data to 1.9 million customers

HealthNet is notifying some 1.9 million customers that personal and health data may have been contained on drives that were found missing from a data center in California.

March 15, 2011 — Computerworld —
THE HEALTHCARE INDUSTRY HAS ONE

7%

of the highest churn rates (7 percent), likely because consumers have higher expectations for the protection and privacy of their most sensitive medical information.
**Not All Publicity Is Good**

**Health Information Privacy**

**Breaches Affecting 500 or More Individuals**

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

**Full DataSet** [CSV format (18 KB)] [XML format (57 KB)]

Select a column head to sort by that column. Select again to reverse the sort order. Select an individual record to display it in full below the table.

| Filter: |
| 435 records showing |

<table>
<thead>
<tr>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Individuals Affected</th>
<th>Date of Breach</th>
<th>Type of Breach</th>
<th>Location of Breached Info</th>
</tr>
</thead>
</table>

© 2012 Protiviti Inc. This document may not be copied nor distributed to any third party.
The HIPAA Audit Timeline

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html
What Will The Audits Look Like?

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html
Additional Forces To Focus On
## Emerging IT Trends

### Demand Side

1. **Rise of the Knowledge Worker**
   - Widespread transaction automation and outsourcing, and the resulting shift in retained skills, mean almost everyone is becoming a knowledge worker.

2. **Ubiquitous Data**
   - The rise of "smart" mobile devices and "ubiquitous sensing" will drive an exponential increase in data volume and throughput.

3. **Social Media**
   - The way customers and consumers learn about products and interact with companies is changing fundamentally.

### Supply Side

4. **Tech-Savvy Workforce**
   - Technology knowledge and confidence in the workforce is broadening but losing its depth (fewer have a deep technical expertise).

5. **Technology as a Service**
   - Infrastructure and applications are becoming available as virtualized, configurable, and scalable services in the cloud (or will) adopt licensing structures to mimic a service.

6. **Desktop Transformation**
   - Virtualization, SaaS, and unified communications combined with greater workforce mobility triggers a "transformation of the desktop," enabling device-agnostic service delivery.

### Organization Side

7. ** Fewer than 25% of employees currently within IT will remain in their current roles**

8. **Several trends in IT demand and supply will change how organizations use technology to create value, and the roles, structure and skills of the IT function**

---

© 2012 Protiviti Inc. This document may not be copied nor distributed to any third party.
Areas of Focus

PwC 2012 Health Research Institute “Top10”

– #3: Providers and insurers team up for population health
  • payer-provider will increase their teaming to integrate care, share information and participate in new payment models with incentives for shared savings.

– #5: Investments in health informatics ramp up. Information is king
  • Before data assets can be maximized, the industry will need to address issues around data collection, quality and integration, develop scalable analytical tools, address privacy and security, and overcome the shortage of skilled informatics professionals and trainers.

– #6. Privacy and security become a billboard for new business.
  • Health organizations will focus more because consumers consider privacy and security issues a differentiator.

– #9. Social media plays a bigger role in healthcare.
  • 32% of all respondents, including half of people under the age of 35, have used social media channels for healthcare purposes, such as connecting with health organizations and other people with shared health interests. Healthcare organizations are experimenting with building stronger connections and communities through social media, and the trend is expected to grow in 2012 as social media becomes part of an organization's overall strategy to improve healthcare and outcomes.
# Stakeholders In The Healthcare Ecosystem

<table>
<thead>
<tr>
<th>Points of Care</th>
<th>Payers</th>
<th>Clinical Support</th>
<th>Business Associates</th>
<th>Others</th>
<th>IT Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Primary care physicians</td>
<td>- Primary insurers</td>
<td>- Clinical labs</td>
<td>- Pharmacy benefits managers</td>
<td>- Life insurance companies</td>
<td>- Data transmission (HIE)</td>
</tr>
<tr>
<td>- Secondary physicians</td>
<td>- Secondary insurers</td>
<td>- Research labs</td>
<td>- Third-party administrators</td>
<td>- Law firms</td>
<td>- Data storage</td>
</tr>
<tr>
<td>- OB/GYN physicians</td>
<td>- Medicare</td>
<td>- Imaging companies</td>
<td>- Benefits administrators</td>
<td>- Consultants</td>
<td>- Data back-up</td>
</tr>
<tr>
<td>- Clinics</td>
<td>- Medicaid</td>
<td>- Pharmacies</td>
<td>- Claims review/ utilization</td>
<td>- Auditors</td>
<td>- Data recovery services</td>
</tr>
<tr>
<td>- Hospitals</td>
<td>- Employers: benefits</td>
<td>- Mail-order pharmacies</td>
<td>- Billing processors</td>
<td>- Accreditation firms</td>
<td>- Software as a service (SaaS)</td>
</tr>
<tr>
<td>- Therapists</td>
<td>administrators</td>
<td>- Phlebotomists</td>
<td>- Revenue cycle companies</td>
<td>- Application trouble-shooters</td>
<td>- On-line diagnostic services</td>
</tr>
<tr>
<td>- Homeopaths</td>
<td>- Consumers</td>
<td></td>
<td>- Payment agencies</td>
<td>- Pharmaceutical/ medical</td>
<td>- Mobile devices</td>
</tr>
<tr>
<td>- Long term care facilities</td>
<td></td>
<td></td>
<td>- Collection agencies</td>
<td>device companies</td>
<td>- Web portals: physicians</td>
</tr>
<tr>
<td>- Rehab facilities</td>
<td></td>
<td></td>
<td>- Hospital discharge care support</td>
<td>- Contract research</td>
<td>- Web portals: consumers</td>
</tr>
<tr>
<td>- Assisted living</td>
<td></td>
<td></td>
<td>- Disease management companies</td>
<td>organizations</td>
<td></td>
</tr>
<tr>
<td>- Urgent care facilities</td>
<td></td>
<td></td>
<td>- Wellness companies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Telehealth/ telemedicine</td>
<td></td>
<td></td>
<td>- Fulfillment companies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Retail physicians</td>
<td></td>
<td></td>
<td>- Health risk assessment organizations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cloud computing is a model for enabling on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction OR simply, “IT runs over the internet instead of installing hardware and software yourself.”

### Characteristics
- On demand self-service
- Pay as you use
- Rapid elasticity (expand / contract)
- Multi tenancy (shared pool)
- Broad network access

### Service Models
- **Business Process as a Service (emerging)**
  Entire business process as a service in the cloud
- **Software as a Service**
  Finished applications that you rent and customize
- **Platform as a Service**
  Developer platform that abstracts the infrastructure, OS, and middleware for developer productivity
- **Infrastructure as a Service**
  Deployment platform that abstracts the infrastructure

### Deployment Models
- Public Cloud
- Community Cloud
- Hybrid Cloud
- Private Cloud
As visibility is lost...

- Where is the data?
- Who can see the data?
- Who has seen the data?
- Has data been tampered with?
- Where is processing performed?
- How is processing configured?
- Does backup happen? How? Where?

... security, compliance, and value are lost as well.
Mobile Commerce – Contextual Mobility

Pre-context

Simple single-vendor systems and walled gardens

Open systems and federations

Device Centric
- Presence, PIM

2009

2010 - 2012

Device Centric
- Location, Identity, Simple behavior and habits
- Location-aware social networks
- Simple proactive alerts

People Centric
- Sensors, bio sensors
- Adjacent devices and people
- Complex anticipatory behavior
- Complex federated services
- Contextual social networking

2015 - 2020

Source: Gartner: Trends and Directions in Mobile and Wireless

© 2012 Protiviti Inc. This document may not be copied nor distributed to any third party.
Virtual doctors visits catch on with insurers, employers

By Phil Galewitz, Kaiser Health News

Tired of feeling "like the walking dead" but worried about the cost of a doctor's visit, Amber Young sat on her bed near tears one recent Friday night in Woodbury, Minn.

That's when she logged onto an Internet site, run by NowClinic online care, a subsidiary of UnitedHealth Group (parent of health insurer UnitedHealthcare), and "met" with a doctor in Texas.

After talking with the physician via instant messaging and then by telephone, Young was diagnosed with an upper respiratory illness and prescribed an antibiotic that her husband picked up at a local pharmacy. The doctor's
Security Trends in Social Media

- 21% accept contact offerings from members they don’t recognize
- More than half let acquaintances or roommates access social networks on their machines
- 64% click on links offered by community members or contacts
- 26% share files within social networks
- 20% have experienced identity theft
- 47% have been victims of malware infections
- Facebook has been hit with malicious applications and new version of the Koobface virus, which allows hackers to steal information from personal profiles
- Huge increase in “likejacking”
Top Risks Associated With These New Technologies

- Regulatory Risk
- IP Loss
- Sensitive Data Loss
- Reputation Risk
- Financial Risk
- Safety Risk
- Personal Reputation Loss
- Lack of Governance
- Litigation Risk
- Infrastructure Stability Risk
- Information Security Risk
At Least The Infrastructure Is Straight-Forward
Healthcare Challenges

- Inconsistency
- Inefficiency
- Increasing Costs
- Greater Risk

- Inability to implement security in devices and applications
- Ineffective and inefficient compliance management
- Limited guidance and inconsistent expectations for security across the industry
- Increasing breaches in the industry
- Greater oversight, scrutiny both internally and externally
- Numerous and ambiguous federal and state regulations
- Rapidly changing business, technology and regulatory environment

- Information Networks
- Device Manufacturers
- Bio-tech firms
- Pharmacies
- Providers
- PBM
- Health Plans
- Third-Party Processors
Ideas For Efficiently Defining Your Risks and Addressing Them
What is HITRUST and the CSF?

- The Health Information Trust Alliance (HITRUST) was born out of the belief that information security should be a core pillar of the broad adoption of health information systems and exchanges.

- Industry-based collaboration among healthcare, business, technology and information security leaders, has established the Common Security Framework (CSF), a certifiable framework that can be used by any and all organizations that create, access, store or exchange personal health and financial information.

- The CSF is an information security framework that harmonizes the requirements of existing standards and regulations, including federal (e.g., HITECH Act and HIPAA), state (e.g., MA 201 CMR 17.00), third party (e.g., PCI and COBIT) and government (e.g., NIST, FTC and CMS).
  - HIPAA is not prescriptive, which makes it difficult to apply and open to interpretation.
  - As a framework, the CSF provides organizations with the needed structure, detail and clarity relating to information security tailored to the industry.

- The CSF is the only framework that is built to provide scalable security requirements based on the different risks and exposures of organizations in the industry.

- The CSF also makes security manageable and practical by prioritizing one-third of the controls in the CSF as a starting point for organizations.

- There is no other relevant resource for healthcare organizations to reference for prioritizing their initiatives and validating their investments in security.
One Framework – Multiple Standards

The CSF provides a valuable framework to assess the security controls in a healthcare environment – and provide a path for continuous improvement. Because it was developed leveraging multiple security standards and regulations, the model provides a convenient single model to leverage for many of your security governance requirements.
Organization—Outline

- The CSF contains
  - 13 Security Control Categories
  - 43 Control Objectives
  - 136 Control Specifications.

- Categories (# of objectives and specifications in parentheses) are:
  - Information Security Management Program (1, 1)
  - Access Control (7, 25)
  - Human Resources Security (4, 9)
  - Risk Management (1, 4)
  - Security Policy (1, 2)
  - Organization of Information Security (2, 11)
  - Compliance (3, 10)
  - Asset Management (2, 5)
  - Physical and Environmental Security (2, 13)
  - Communications and Operations Management (11, 33)
  - Information Systems Acquisition, Development and Maintenance (6, 13)
  - Information Security Incident Management (2, 5)
  - Business Continuity Management (1, 5)
## General Information

**Control Reference:** 11.1 Reporting Information Security Events

**Control Specification:** Information security events shall be reported through appropriate communications channels as quickly as possible. All employees, contractors, and third party users shall be made aware of their responsibility to report any information security events as quickly as possible.

*Required for HITRUST Certification 2009*

**Factor Type:** Organizational

## Level 1 Implementation Requirement

### Level 1 Organizational Factors:
- Diotech Organizations: < $100,000 Spend on Research and Development Per Year
- Pharmaceutical Companies: < 20,000,000 Prescriptions Per Year
- Third Party Processor: < 1,000,000 Records Processed Per Year
- Physician Practice: < 22,000 Visits Per Year
- Medical Facilities / Hospitals: < 1,000 Licensed Beds
- Health Plan / Insurance: < 1,000,000 Covered Lives

### Level 1 Regulatory Factors:
- None

**Level 1 Implementation:**

Formal information security event reporting procedures to support the corporate direction (policy) shall be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event, and the timeliness of reporting and response. With the importance of information Security incident handling, a policy shall be established to set the direction of management.

A point of contact shall be established for the reporting of information security events. It shall be ensured that this point of contact is known throughout the organization, is always available and is able to provide adequate and timely response.

**Level 1 Control Audit Procedures:**

1. The organization’s information security policy to ensure information security event reporting procedures that support the corporate direction have been established.
2. The organization’s information security policy to ensure an incident response and escalation procedure is defined, setting out the action to be taken on receipt of a report of an information security event, and the timeliness of reporting and response.
3. The organization’s information security policy to ensure it defines the direction of management.
4. The organization’s information security policy and/or organization chart to a point of contact has been established for the reporting of information security events.

**Interview:**

1. Management to verify the direction of the organization relating to information security and incident reporting, response and escalation is aligned with the policy.
2. Select a member of the organization who has responsibility for incident reporting to verify that he/she has a clear understanding of the policy and procedures.

**Test:**

- None

**Level 1 Control Standard Mapping:**

- HIPAA §164.312 (a)(8)(ii)

## Level 1 Alternate Controls

<table>
<thead>
<tr>
<th>Control Name</th>
<th>Control Type</th>
<th>Control Description</th>
</tr>
</thead>
</table>
| No records specified.
Sample Deliverables

Risk Assessment Results

Organizational and System Control Requirement Summary

<table>
<thead>
<tr>
<th>Control</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1. a User Registration</td>
<td>Partial</td>
<td>Partial</td>
<td>Partial</td>
</tr>
<tr>
<td>3.1. b User Authentication</td>
<td>In Place</td>
<td>In Place</td>
<td>In Place</td>
</tr>
<tr>
<td>3.1. c Multiple Access Management</td>
<td>In Place</td>
<td>In Place</td>
<td>In Place</td>
</tr>
<tr>
<td>3.1. d User Password Management</td>
<td>Partial</td>
<td>In Place</td>
<td>Partial</td>
</tr>
<tr>
<td>3.1. e Review of User Access Rights</td>
<td>In Place</td>
<td>Not In Place</td>
<td></td>
</tr>
<tr>
<td>3.1. f Access Identification in Networks</td>
<td>In Place</td>
<td>In Place</td>
<td>In Place</td>
</tr>
<tr>
<td>3.1. g Secure Logon Procedures</td>
<td>Partial</td>
<td>Partial</td>
<td>Not In Place</td>
</tr>
<tr>
<td>3.1. h User Identification and Authentication</td>
<td>In Place</td>
<td>Not In Place</td>
<td></td>
</tr>
<tr>
<td>3.1. i Password Management System</td>
<td>In Place</td>
<td>In Place</td>
<td>In Place</td>
</tr>
<tr>
<td>3.1. j Use of System Utilities</td>
<td>In Place</td>
<td>In Place</td>
<td>Partial</td>
</tr>
<tr>
<td>3.1. k Session Timeout</td>
<td>Partial</td>
<td>Partial</td>
<td>Partial</td>
</tr>
<tr>
<td>3.1. l Limitation of Connection Time</td>
<td>Not In Place</td>
<td>Partial</td>
<td>Not In Place</td>
</tr>
<tr>
<td>3.1. m Information Access Restriction</td>
<td>In Place</td>
<td>In Place</td>
<td>Not In Place</td>
</tr>
<tr>
<td>3.1. n Access to System Location</td>
<td>In Place</td>
<td>In Place</td>
<td>In Place</td>
</tr>
<tr>
<td>3.1. o Mobile Computing and Communications</td>
<td>In Place</td>
<td>In Place</td>
<td>In Place</td>
</tr>
<tr>
<td>3.1. p Documented Operations Procedures</td>
<td>Partial</td>
<td>Partial</td>
<td>Partial</td>
</tr>
</tbody>
</table>

Road Map

Common Health Information Protection Questionnaire (CHIP)

Executive Summary: HITRUST CSF Gap Assessment Results Summary

<table>
<thead>
<tr>
<th>System 1</th>
<th>System 2</th>
<th>System 3</th>
<th>System 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>In Place</td>
<td>16 10 3</td>
<td>12 7 0</td>
<td>18 12 3</td>
</tr>
<tr>
<td>Partial</td>
<td>6 6 1</td>
<td>9 6 0</td>
<td>9 5 0</td>
</tr>
<tr>
<td>Not In Place</td>
<td>6 9 4</td>
<td>9 11 2</td>
<td>6 2 1</td>
</tr>
</tbody>
</table>
Overview of CSF Assurance Program

- Utilizes a common set of information security requirements with standardized assessment and reporting processes accepted and adopted by healthcare organizations.
- Through the program, healthcare organizations and their business associates can improve efficiencies and reduce the number and costs of security assessments.
- The oversight and governance provided by HITRUST support a process whereby organizations can trust that their third parties have essential security controls in place.
Healthcare Challenges

Healthcare organizations are facing multiple challenges with regards to information security:

- Costs and complexities of redundant and inconsistent requirements and standards
- Critical systems not incorporating appropriate controls or safeguards
- Confusion around implementation and acceptable baseline controls
- Information security audits subject to different interpretations of control objectives and safeguards
- Increasing scrutiny and similar queries from regulators, auditors, underwriters, customers and business partners
- Growing risk and liability
In Summary

• HITRUST Common Security Framework (CSF) Provides:
  – A scalable and flexible approach designed by your peers,
  – A prescriptive and specific set of meaningful security controls,
  – A comprehensive view of any healthcare organization and ecosystem, and
  – An efficient methodology with certifiable and reusable results.
  
  → The best alternative available to understand and communicate your information security posture.

• As Audit Professionals We Should:
  – Leverage insightful and repeatable audit approaches.
  – Be involved early in discussions on new technologies (especially Cloud and Social Media).
  – Be the voice of reason on risk and possible mitigation approaches.

• Refine Your Crisis Management Plan
  – Ensure the right people/roles are “at the table”.
  – Reflect data breach notification requirements.
  – Integrate the risks associated with new technologies.
Thank You

Cal Slemp
Managing Director
New York, NY
+1.203.905.2926
cal.slemp@protiviti.com
Additional HITRUST Resources

Visit HITRUSTalliance.net for information and materials on:

- Common Security Framework - www.hitrustalliance.net/csf/
- CSF Assurance Program - www.hitrustalliance.net/assurance/
Access to the CSF online.

A professional network for:

- Understanding industry issues and events
- Sharing knowledge
- Exchanging ideas and best practices
- Discovering new ways to solve business problems
- Downloading documentation and training materials

Providing support:

- What does this control mean?
- How do I implement these requirements?
- What do I do if I cannot meet a requirement?
Some Information

- Adoption of the CSF
  - Hospitals\(^1\) 62%
  - Health Plans\(^2\) 74%
- Adoption of the CSF Assurance Program
  - Assessments requested of Partners in Jan 2011 11,000
- Regional User Group Chapters (monthly) 5
- CSF Assessors 12
- HITRUST Central Community Members 5,000+
- Trained CSF Practitioners\(^3\) 200

---

1 – Based on facilities in the 2009 AHA hospital and health system data as of Dec 2010
2 – Based on health plans with over 500,000 members as of Dec 2010
3 – Every training class (5 day class) is full through June 2011
Existing Standards and Regulations Coverage

WHAT

- HIPAA Security
- HITECH Act
- Mngfl. Use*
- PCI
- ISO 27001/2
- NIST 800-53
- States

HOW

SCOPE OF COVERAGE

*Meaningful Use Requirements
## CSF Versus Other Standards

<table>
<thead>
<tr>
<th>Requirement</th>
<th>CSF</th>
<th>COBIT</th>
<th>PCI</th>
<th>ISO</th>
<th>NIST</th>
<th>HIPAA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehensive – general security</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Partial</td>
</tr>
<tr>
<td>Comprehensive – regulatory, statutory, and business security requirements</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Prescriptive</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Partial</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Practical and scalable</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Audit or assessment guidelines</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Certifiable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No*</td>
<td>No</td>
</tr>
<tr>
<td>Support for third-party assurance</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Open and transparent update process</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cost</td>
<td>Free</td>
<td>Free</td>
<td>Free</td>
<td>Subsc.</td>
<td>Free</td>
<td>Free</td>
</tr>
</tbody>
</table>