IIABA ACT Briefing
HIPAA-HITECH Requirements

May 11, 2012

Bob Chaput, MA, CISSP, CHP, CHSS, MCSE
615-656-4299 or 800-704-3394
bob.chaput@ClearwaterCompliance.com
Clearwater Compliance LLC

Bob Chaput

CISSP, MA, CHP, CHSS, MCSE

- President – Clearwater Compliance LLC
- 30+ years in Business, Operations and Technology
- 20+ years in Healthcare
- Executive | Educator |Entrepreneur
- Global Executive: GE, JNJ, HWAY
- Responsible for largest healthcare datasets in world
- Numerous Technical Certifications (MCSE, MCSA, etc)
- Expertise and Focus: *Healthcare, Financial Services, Legal*

- Member: NMGMA, HIMSS, ISSA, HCCA, ACHE, AHIMA, NTC, ACP, Chambers, Boards

http://www.linkedin.com/in/BobChaput

About HIPAA-HITECH Compliance

1. We are not attorneys!

2. HIPAA and HITECH is dynamic!

3. Lots of different interpretations!

So there!

Briefing Objectives

1. Understand “The Problem”
2. Review Necessary Actions
3. Appreciate Expected Outcomes

Why is This Man Smiling?

"…only way to change is through enforcement…"

"…our 5% budget reduction doesn't change anything…"

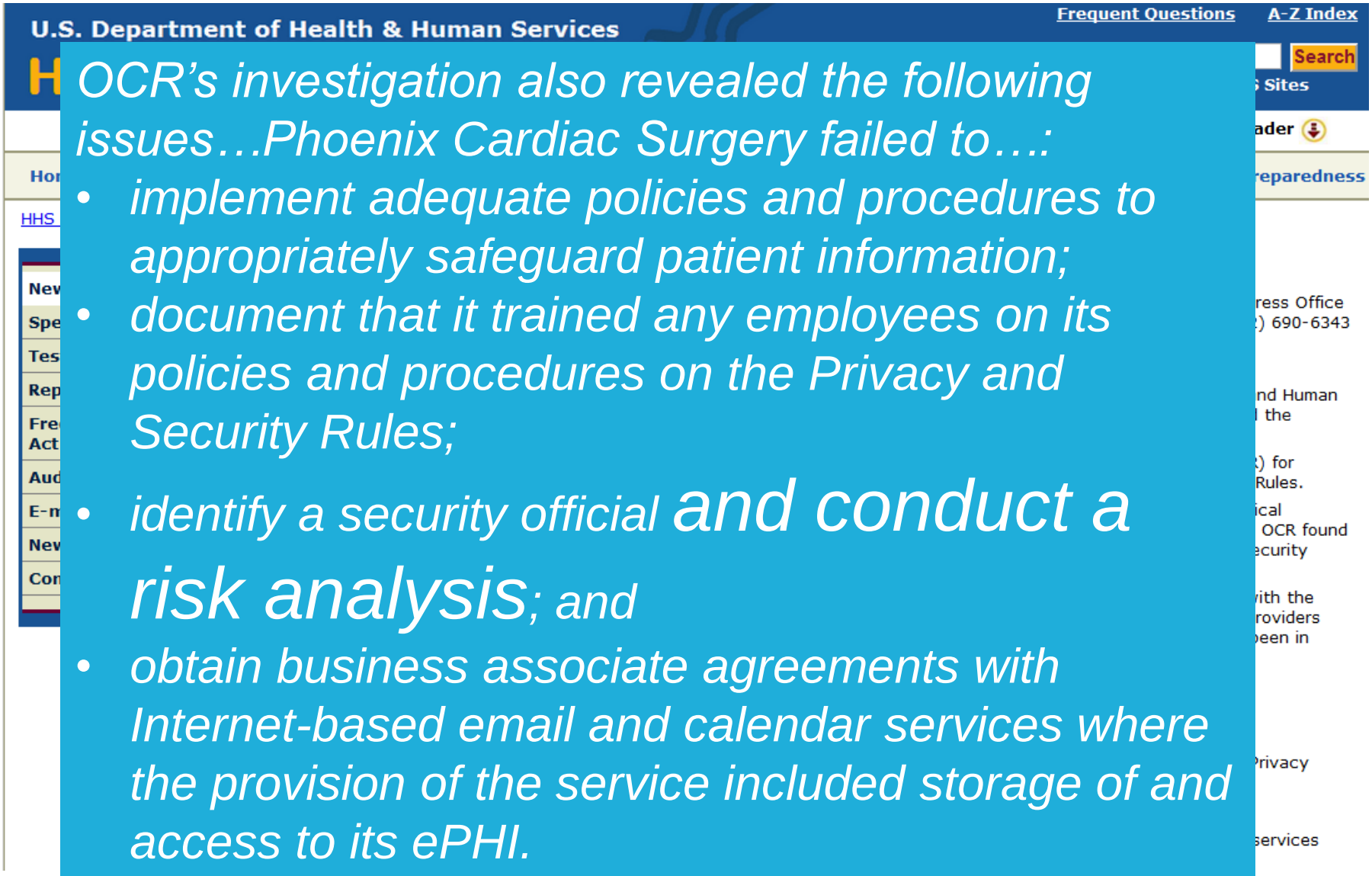
"… enforcement revenues will be used for restitution for victims…AND… reinvestment in STRATEGIC ENFORCEMENT…"

"… enforcement will continue and intensify…"

"…we're moving from complaint-driven to proactive enforcement…"

"… we're looking for the "whole menu"…get going on training, PnPs and risk analysis…"

HHS Snags Small One - $100K



OCR's investigation also revealed the following issues…Phoenix Cardiac Surgery failed to…:

- *implement adequate policies and procedures to appropriately safeguard patient information;*
- *document that it trained any employees on its policies and procedures on the Privacy and Security Rules;*
- *identify a security official* ***and conduct a risk analysis****; and*
- *obtain business associate agreements with Internet-based email and calendar services where the provision of the service included storage of and access to its ePHI.*

Why is VITO[1] NOT Really Smiling?

Chief Executive Officer and Associate Vice Chancellor, Dr. David T. Feinberg, M.D., M.B.A.

3

4

SecurityFocus™ About Contact

Run your small business. We'll protect it.
Complete protection solution designed for small business.
More Info

PRINT EMAIL COMMENT (page 1 of 2) next

UCLA alerts 800,000 to data
Robert Lemos, SecurityFocus 2006-12-12

The University of California, Los A
risk of identity fraud after an unkr
information on approximately 80

UCLA patient data breached (again)

November 7, 2011 — 1:27pm ET | By Karen M. Cheung

+1 0 Like

TOOLS
Subscribe
Email
Print
Contact Author
Reprint

TAGS
data breach
External Hard Drive
medical records
UCLA

A piece of paper with the password to personal information of 16,288 patients is missing after a home invasion of a former employee. UCLA Health System on Friday notified the thousands of at-risk patients that an external hard drive containing the encrypted information was stolen in September.

Although the health system says there are no reported misuses or accessed information following the incident, the information included first and last names and may have included birth dates, medical record numbers, addresses, and medical record information. The information did not include Social Security numbers or any financial information, according to an UCLA statement.

ses
ts
cal

decisions, staying on the right side of all relevant governmental regulations and the law

[1]Very Important Top Official

Mega Session Objective

Help You Understand and Address Two Very Specific HIPAA-Security Compliance Assessments… and, Advise You to Assess Privacy and Breach Notification!!

Why Should You Care?

1. It's the law… HIPAA & HITECH!

2. Your stakeholders trust and expect you to do this

3. Your revenues, assets and reputation depends on it!

PART 1—IMPROVED PRIVACY PROVISIONS AND SECURITY PROVISIONS

42 USC 17931.

SEC. 13401. APPLICATION OF SECURITY PROVISIONS AND PENALTIES TO BUSINESS ASSOCIATES OF COVERED ENTITIES; ANNUAL GUIDANCE ON SECURITY PROVISIONS.

(a) APPLICATION OF SECURITY PROVISIONS.—Sections 164.308, 164.310, 164.312, and 164.316 of title 45, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity. The additional requirements of this title that relate to security and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity.

(b) APPLICATION OF CIVIL AND CRIMINAL PENALTIES.—In the case of a business associate that violates any security provision specified in subsection (a), sections 1176 and 1177 of the Social Security Act (42 U.S.C. 1320d–5, 1320d–6) shall apply to the business associate with respect to such violation in the same manner such sections apply to a covered entity that violates such security provision.

(c) ANNUAL GUIDANCE.—For the first year beginning after the date of the enactment of this Act and annually thereafter, the Secretary of Health and Human Services shall, after consultation with stakeholders, annually issue guidance on the most effective and appropriate technical safeguards for use in carrying out the sections referred to in subsection (a) and the security standards in subpart C of part 164 of title 45, Code of Federal Regulations, including the use of standards developed under section 3002(b)(2)(B)(vi) of the Public Health Service Act, as added by section 13101 of this Act, as such provisions are in effect as of the date before the enactment of this Act.

42 USC 17934.

SEC. 13404. APPLICATION OF PRIVACY PROVISIONS AND PENALTIES TO BUSINESS ASSOCIATES OF COVERED ENTITIES.

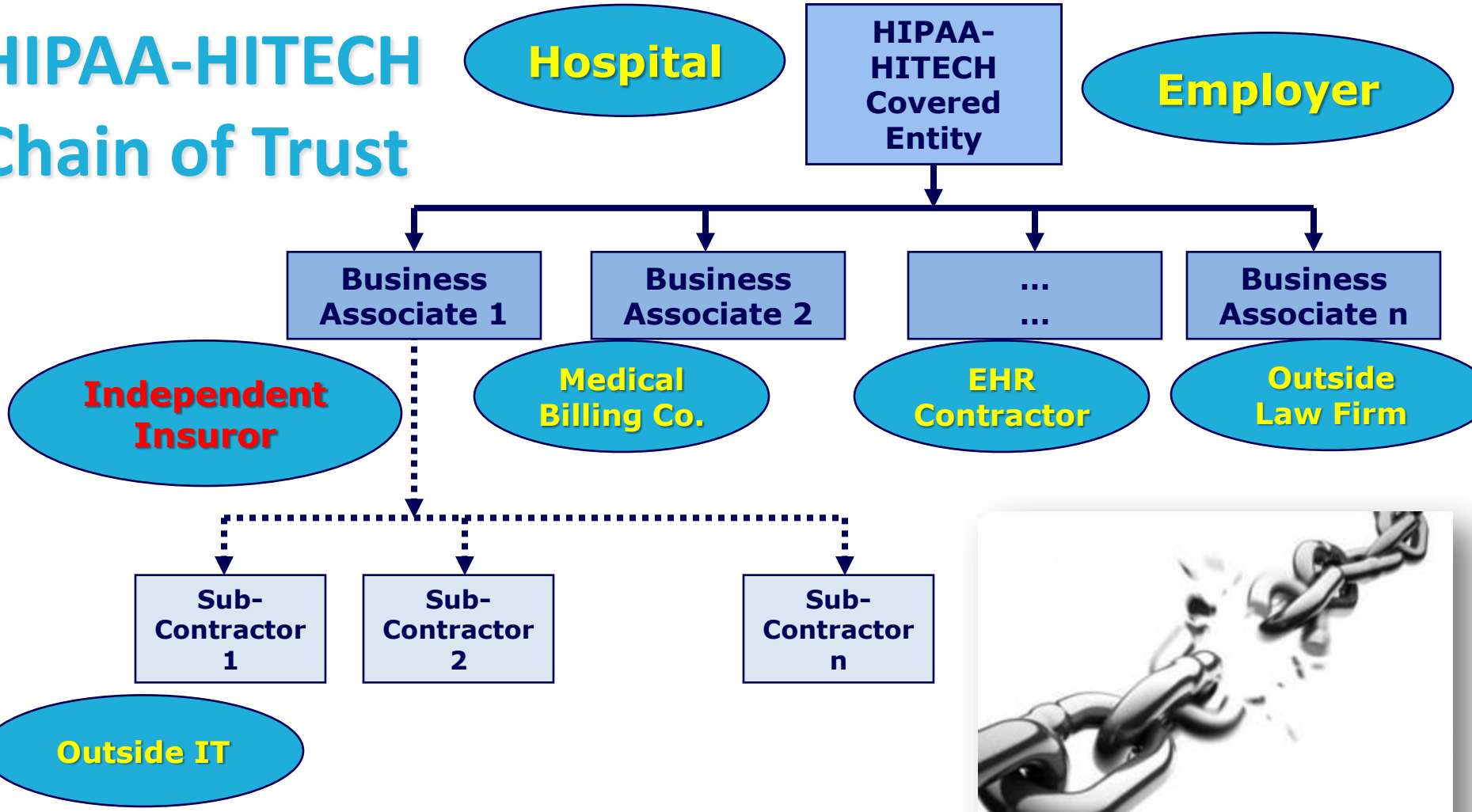
Business Associates

(a) APPLICATION OF CONTRACT REQUIREMENTS.—In the case of a business associate of a covered entity that obtains or creates protected health information pursuant to a written contract (or other written arrangement) described in section 164.502(e)(2) of title 45, Code of Federal Regulations, with such covered entity, the business associate may use and disclose such protected health information only if such use or disclosure, respectively, is in compliance with each applicable requirement of section 164.504(e) of such title. The additional requirements of this subtitle that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity.

(b) APPLICATION OF KNOWLEDGE ELEMENTS ASSOCIATED WITH CONTRACTS.—Section 164.504(e)(1)(ii) of title 45, Code of Federal Regulations, shall apply to a business associate described in subsection (a), with respect to compliance with such subsection, in the same manner that such section applies to a covered entity, with respect to compliance with the standards in sections 164.502(e) and 164.504(e) of such title, except that in applying such section 164.504(e)(1)(ii) each reference to the business associate, with respect to a contract, shall be treated as a reference to the covered entity involved in such contract.

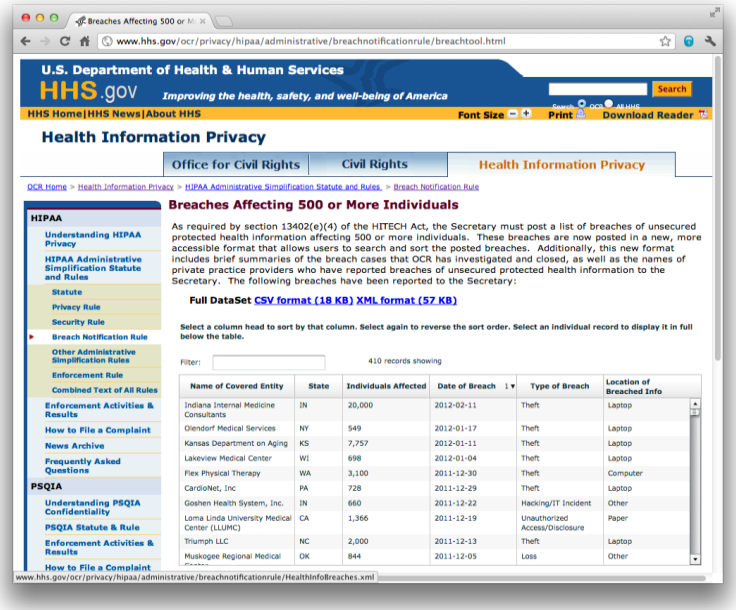
(c) APPLICATION OF CIVIL AND CRIMINAL PENALTIES.—In the case of a business associate that violates any provision of subsection (a) or (b), the provisions of sections 1176 and 1177 of the Social Security Act (42 U.S.C. 1320d–5, 1320d–6) shall apply to the business associate with respect to such violation in the same manner as such provisions apply to a person who violates a provision of part C of title XI of such Act.

HIPAA-HITECH Chain of Trust



Regulations Create Chain of Trust

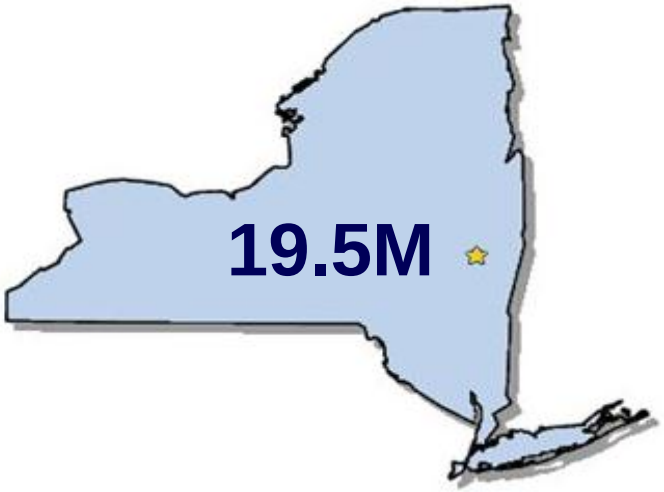
"HHS Wall of Shame"



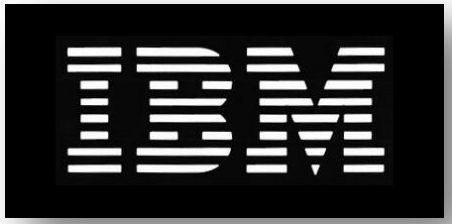
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

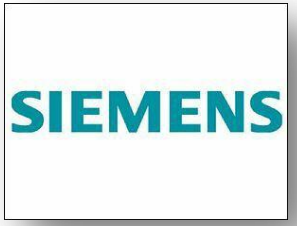
04-26-2012
- 421 CEs
- 89 Named BAs

~19.2M Individuals
Or State of NY



What do they have in common?





Legal Activity

- BCBS Tennessee to pay $1.5 million in HIPAA settlement
- Sutter Health Hit With $1B Class-Action Lawsuit
- Patient files $20M lawsuit against Stanford Hospital
- TRICARE Health Management Sued for $4.9B
- UCLA Health System Enters into $865K Resolution Agreement & CAP with OCR
- Cignet Health Fined for Violation of HIPAA Privacy Rule: $4.3M
- MGH entering into a resolution agreement; includes a $1 million settlement

- AvMed Health sued over 'one of the largest medical breaches in history'
- Health Net keeps paying for its data breach in 2009… $625K and counting
- WellPoint's notification delay following data breach brings action by Attorney General's office

Lawsuits and Enforcement are on the upswing…

THE WALL STREET JOURNAL.
WSJ.com

March 12, 2012, 12:39 PM ET

Burglary Triggers Medical Records Firm's Collapse

The New Year's Eve burglary of a California office building has led to the collapse of a national medical records firm.

Impairment Resources LLC filed for bankruptcy Friday after the break-in at its San Diego headquarters led to the electronic escape of detailed medical information for roughly 14,000 people, according to papers filed in U.S. Bankruptcy Court in Wilmington, Del. That information included patient addresses, social security numbers and medical diagnoses.

Police never caught the criminals, and company executives were required by law to report the breach to state attorneys general and the Department of Labor's Office of Inspector General. Some of those agencies, including the Department of Labor, are still investigating the matter, the company said in court papers.

"The cost of dealing with the breach was prohibitive" for the company, Impairment Resources said when explaining its decision to file for Chapter 7 bankruptcy protection. That type of bankruptcy is used most often by companies to shut down and sell off what's left to pay off their debts.

Getting serious…?

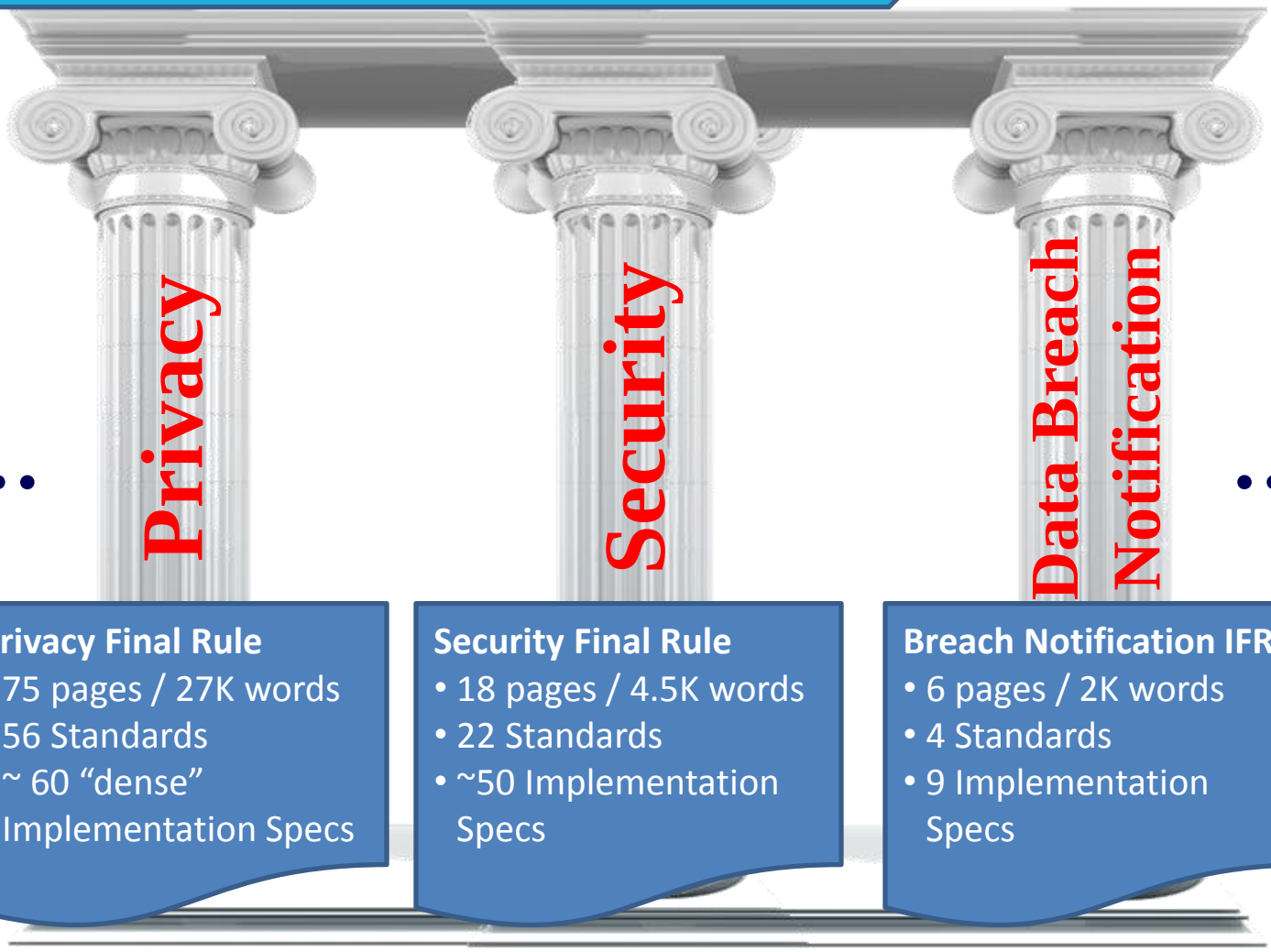
Briefing Objectives

1. Understand “The Problem”
2. Review Necessary Actions
3. Appreciate Expected Outcomes

Three Pillars of HIPAA-HITECH Compliance…

HITECH

HIPAA



Privacy Final Rule
- 75 pages / 27K words
- 56 Standards
- ~ 60 "dense" Implementation Specs

Security Final Rule
- 18 pages / 4.5K words
- 22 Standards
- ~50 Implementation Specs

Breach Notification IFR
- 6 pages / 2K words
- 4 Standards
- 9 Implementation Specs

7 Actions to Take Now

1. Privacy and Security Risk Management & Governance Program (45 CFR § 164.308(a)(1))
2. Complete a HIPAA Security Evaluation (45 CFR § 164.308(a)(8))

3. Complete a HIPAA Security Risk Analysis (45 CFR § 164.308(a)(1)(ii)(A))
4. Develop comprehensive HIPAA Privacy and Security and Breach Notification Policies & Procedures (45 CFR § 164.530 and 45 CFR § 164.316)
5. Complete a Privacy Rule compliance assessment (45 CFR § 164.530)
6. Complete a Breach Rule compliance assessment (45 CFR § 164.400)
7. Document and act upon a corrective action plan

Use the Regulations as Checklists!

Assessments and Audits Are Central to Compliance

- Establishing good policy and procedures is not enough…
- Comprehensive business processes are not enough…
- Deploying leading technology solutions and systems controls is not enough…

Regular assessments are crucial in establishing and maintaining effective compliance

Security Evaluation v. Risk Analysis

45 C.F.R. § 164.308(a)(8)

Standard: Evaluation. Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, **which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.**

NOT SUFFICIENT TO CALL THE 'GEEK SQUAD' TO RUN A VULNERABILITY SCAN OR PENETRATION TEST…

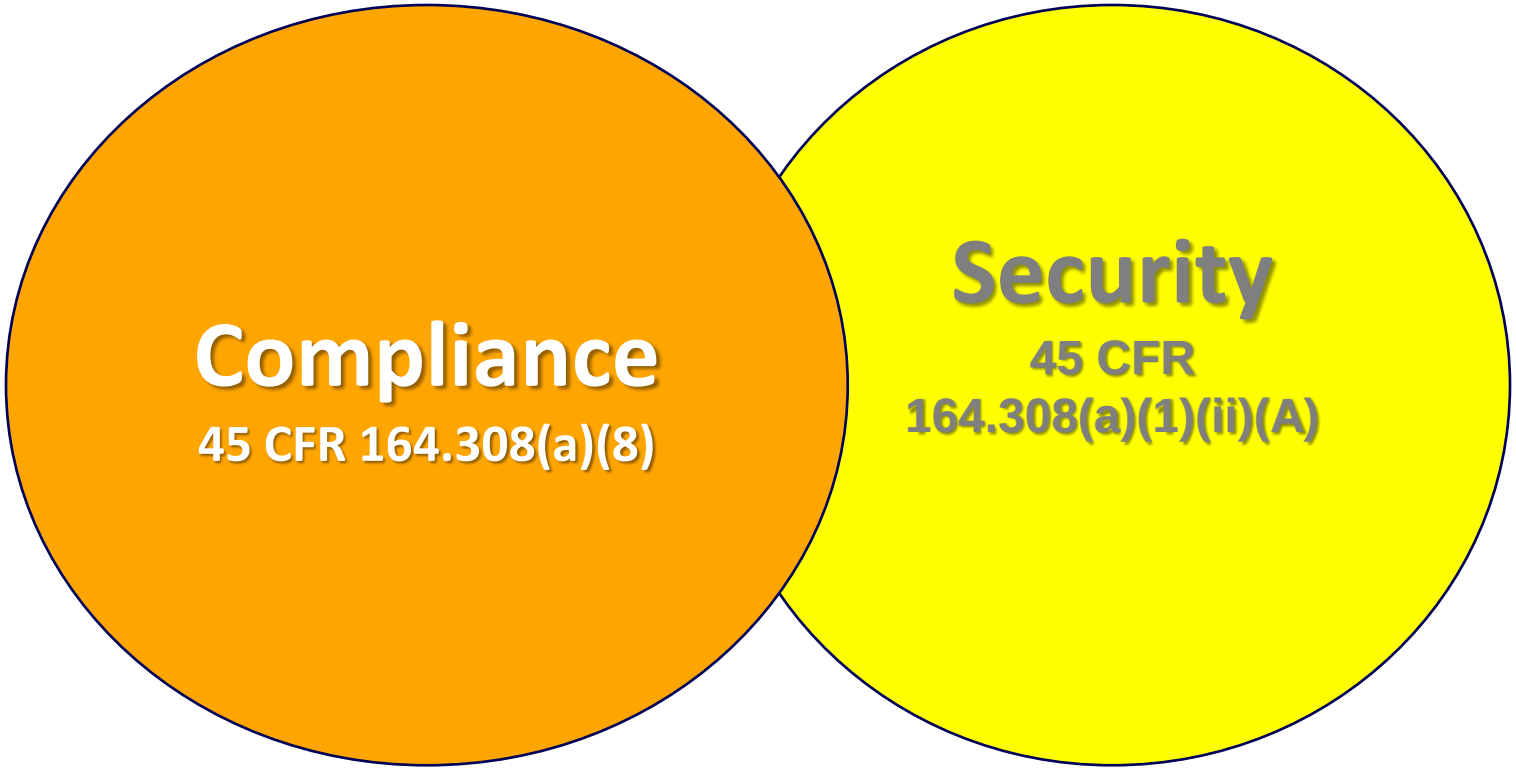
45 C.F.R. § 164.308(a)(1)(i) Standard: Security Management Process

(1)(i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) Implementation specifications:

(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

Two Dimensions of HIPAA Security Business Risk Management



Overall Business Risk Management Program;
Not "an IT project"

Briefing Objectives

1. Understand “The Problem”
2. Review Necessary Actions
3. Appreciate Expected Outcomes

Balanced Privacy & Security Program

Policy defines an organization's values & expected behaviors.

Procedures or process provide the actions required to deliver on organization's values.

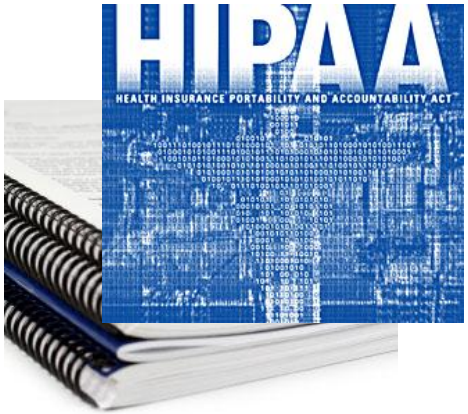
People must include talented privacy & security & technical staff, supportive management and trained/aware colleagues.

Technology includes the various families of technical security controls including encryption, firewalls, antivirus, intrusion detection, AND Incident management tools

3 Dimensions of HIPAA

Security Evaluation

1. **Is it documented?**
   - Policies, Procedures and Documentation



2. **Are you doing it?**
   - Using, Applying, Practicing, Enforcing

3. **Is it Reasonable and Appropriate?**
   - Comply with the implementation specification

…from HHS/OCR Final Guidance

Regardless of t…ployed…

1. **Scope of the An…**
   must be included in the …
2. **Data Collection …**
   C.F.R. §§ 164.308(a)(1)(ii…
3. **Identify and Doc…**
   Organizations must iden…
   164.306(a)(2), 164.308(a…
4. **Assess Current S…**
   uses to safeguard ePHI. (…
5. **Determine the L…**
   account the likelihood of…
6. **Determine the P…**
   "criticality," or impact, of…
7. **Determine the L…**
   the likelihood of threat o…
   164.308(a)(1)(ii)(A), and …
8. **Finalize Docume…**
   format. (See 45 C.F.R. §…
9. **Periodic Review…**
   order for an entity to up…
   continuous risk analysis to identify when updates are needed. (45 C.F.R. § § 164.306(e) and 164.316(b)(2)(iii).)

…s, or transmits

…nted. (See 45

…s -
…C.F.R. §§

…ument the security measures an entity
…(b)(1).)

…e requires organizations to take into

…le also requires consideration of the
… (See 45 C.F.R. § 164.306(b)(2)(iv).)

…mple, by analyzing the values assigned to
…R. § § 164.306(a)(2),

…cumented but does not require a specific

…k analysis process should be ongoing. In
…ule requires, it should conduct

Guidance on Risk Analysis Requirements under the HIPAA Security Rule

Introduction

The Office for Civil Rights (OCR) is responsible for issuing annual guidance on the provisions in the HIPAA Security Rule.[1] (45 C.F.R. §§ 164.302 – 318.) This series of guidances will assist organizations[2] in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to secure electronic protected health information (e-PHI). The guidance materials will be developed with input from stakeholders and the public, and will be updated as appropriate.

We begin the series with the risk analysis requirement in § 164.308(a)(1)(ii)(A). Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a risk analysis is foundational, and must be understood in detail before OCR can issue meaningful guidance that specifically addresses safeguards and technologies that will best protect electronic health information.

The guidance is not intended to provide a one-size-fits-all blueprint for compliance with the risk analysis requirement. Rather, it clarifies the expectations of the Department for organizations working to meet these requirements.[3] An organization should determine the most appropriate way to achieve compliance, taking into account the characteristics of the organization and its environment.

We note that some of the content contained in this guidance is based on recommendations of the National Institute of Standards and Technology (NIST). NIST, a federal agency, publishes freely available material in the public domain, including guidelines.[4] Although only federal agencies are required to follow guidelines set by NIST, the guidelines represent the industry standard for good business practices with respect to standards for securing e-PHI. Therefore, non-federal organizations may find their content valuable when developing and performing compliance activities.

All e-PHI created, received, maintained or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to

[1] Section 13401(c) of the Health Information Technology for Economic and Clinical (HITECH) Act.
[2] As used in this guidance the term "organizations" refers to covered entities and business associates. The guidance will be updated following implementation of the final HITECH regulations.
[3] The HIPAA Security Rule: Health Insurance Reform: Security Standards, February 20, 2003, 68 FR 8334.
[4] The 800 Series of Special Publications (SP) are available on the Office for Civil Rights' website – specifically, *SP 800-30 - Risk Management Guide for Information Technology Systems.* (http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html.)

Posted July 14, 2010 Page 1

2 Dimensions of HIPAA Security

Risk Management

1. What is our exposure of our information assets (e.g., ePHI)?

2. What do we need to do to treat or manage risks?

A Risk Analysis Addresses Both

Briefing Objectives

1. Understand “The Problem”
2. Review Necessary Actions
3. Appreciate Expected Outcomes

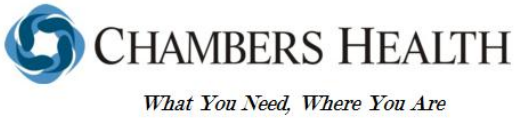
Typical Outcomes

1. Prepare for Mandatory Audits
2. Establish Governance
3. Objective, Independent 3rd Party Review
4. Solid Educational Foundation
5. Completion of 45 CFR 164.308(a)(8) - Evaluation
6. Completion of 45 CFR 164.308(a)(1)(ii)(A) - Risk Analysis
7. Revitalize Security Compliance Program
8. Determine Baseline/Benchmark Score
9. Document Findings, Observation & Recommendations Reports
10. Develop Policies & Procedures
11. Training

Southern Insurance Services, Inc.

1. Business
   - Southern Insurance Services - Lawrenceburg, TN
   - ~10 employees / 30 years in business
   - Marketing Medicare Products to independent agents across the nation for large health plans
   - Periodically received ePHI when troubleshooting claims issues for agents
2. "Problem"
   - **Large Health Plan supplier (Humana) requested HIPAA compliance self-assessment**
   - Required to populate the vendor's eGRC web portal
   - Contacted outside legal that contacted Clearwater Compliance for security-specific help
3. Actions Taken
   - Accelerated, remote HIPAA Security Assessment WorkShop
   - Purchased Clearwater Compliance Security PnPs
   - Modified PnPs to environment
   - Recommended immediate risk remediation steps
   - Assisted answering questions in eGRC portal
4. Outcomes
   - Gained clear understand of HIPAA Security Rule
   - Established Security PnPs
   - Improved control environment
   - Satisfied health plan self-assessment requirements

Selected Clearwater Compliance Clients

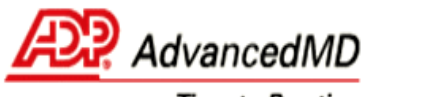


Selected Clearwater Compliance Clients

Selected Clearwater Compliance Clients

Selected Clearwater Compliance Clients

Business Associates / Subcontractors



CLEARWATER COMPLIANCE

Business Associates / Subcontractors

Summary and Next Steps

1. Assess the Forest **First**, Then Get Into the Trees/Weeds

2. Stay Business Risk Management-Focused

3. Large or Small: Get Help (Tools, Experts, etc)

Upcoming HIPAA-HITECH Webinars

Register Now! … at:

http://abouthipaa.com/webinars/upcoming-live-webinars/

Contact

Bob Chaput, CISSP

http://www.ClearwaterCompliance.com
bob.chaput@ClearwaterCompliance.com

Phone: 800-704-3394 or 615-656-4299

Clearwater Compliance LLC

join our LinkedIn group

CERTIFIED HIPAA PROFESSIONAL
HIPAA ACADEMY

CERTIFIED HIPAA SECURITY SPECIALIST™
HIPAA ACADEMY

Additional Information

Get Smart!

"On Demand" HIPAA HITECH RESOU

1. http://AboutHIPAA.com/about-hipaa/resources/
2. http://AboutHIPAA.com/webinars/

Clearwater Co-Sponsored Seminal Report

http://webstore.ANSI.org/PHI

Our Passion

We're excited about what we do because…

…we're helping organizations safeguard the very personal and private healthcare information of millions of fellow Americans…

… And, keeping those same organizations off the Wall of Shame…!

Why Now? – What We're Hearing

"Our business partners (health plans) are demanding we become compliant…" **– large national care management company (BA)**

"We did work on Privacy, but have no idea where to begin with Security" – **6-Physician Pediatric Practice (CE)**

"We want to proactively market our services by leveraging our HIPAA compliance status …" -- **large regional fulfillment house (BA)**

"With all the recent changes and meaningful use requirements, we need to make sure we meet all The HITECH Act requirements …" **– large family medicine group practice (CE)**

"We need to have a way to quickly take stock of where we are and then put in place a dashboard to measure and assure our compliance progress…" **– national research consortium (BA)**

"We need to complete HIPAA-HITECH due diligence on a potential acquisition and need a gap analysis done quickly and efficiently…" **– seniors care management company (BA)**

What Our Customers Say…

"The WorkShop™ process made a very complicated process and subject matter simple. The ToolKit™ itself was excellent and precipitated exactly the right discussion we needed to have." – **outside Legal Counsel, national research consortium**

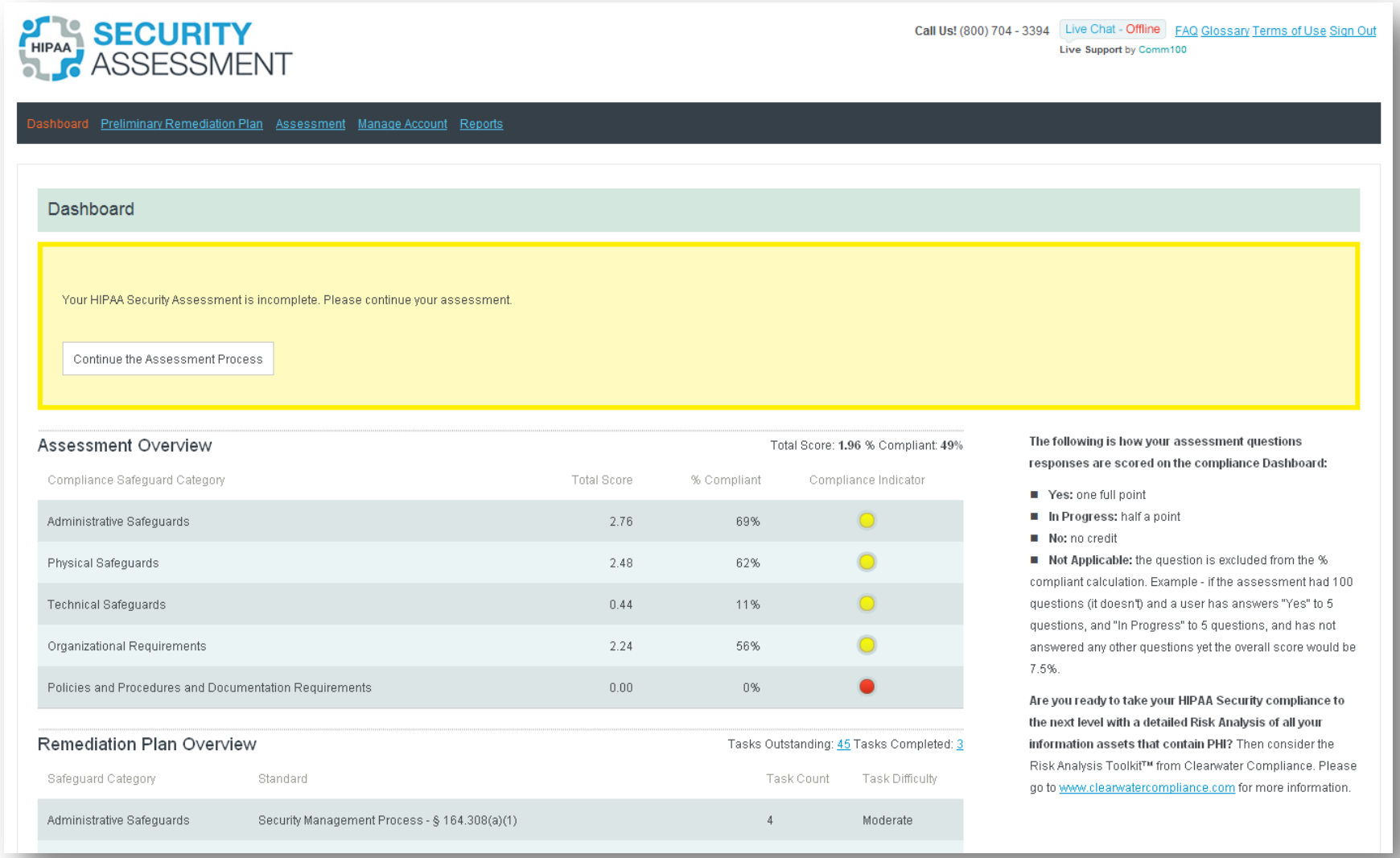
"The HIPAA Security Assessment ToolKit™ and WorkShop™ are a comprehensive approach that effectively guided our organization's performance against HIPAA-HITECH Security requirements." -- **SVP and Chief Compliance, national hospice organization**

"… The WorkShop™ process expedited assessment of gaps in our HIPAA Security Compliance program, began to address risk mitigation tasks within a matter of days and… the 'ToolKit' was a sound investment for the company, and I can't think of a better framework upon which to launch compliance efforts." – **VP & CIO, national care management organization**

"…the process of going through the self-assessment WorkShop™ was a great shared learning experience and teambuilding exercise. In retrospect, I can't think of a better or more efficient way to get started than to use the HIPAA Security Assessment ToolKit." – **CIO, national kidney dialysis center firm**

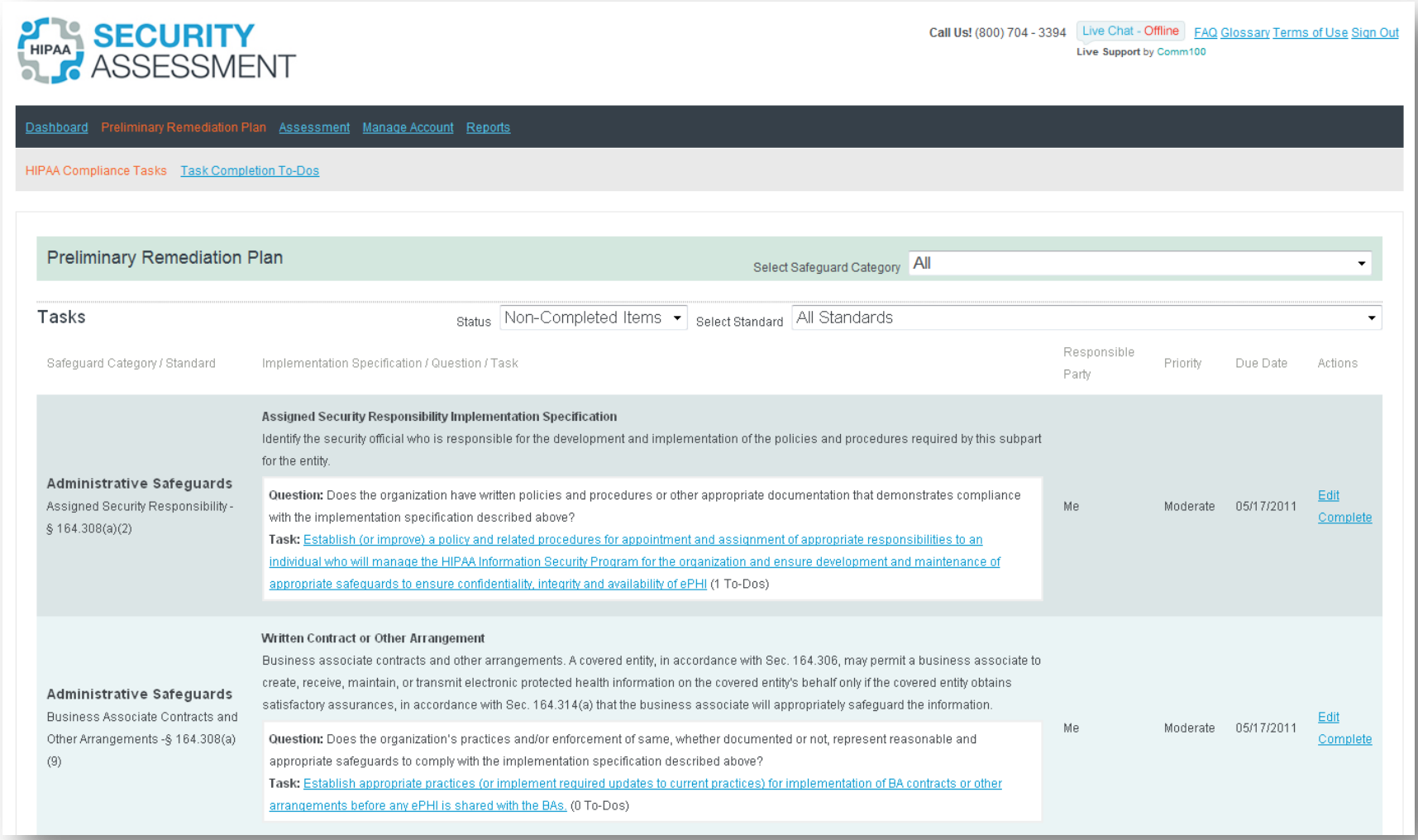
"…this HIPAA Security Assessment Toolkit is worth its weight in gold. If we had to spend our time and resources creating this spreadsheet, we would never complete our compliance program on time…" **— Director, Quality Assurance & Regulatory Affairs**

CLEARWATER COMPLIANCE Dashboard

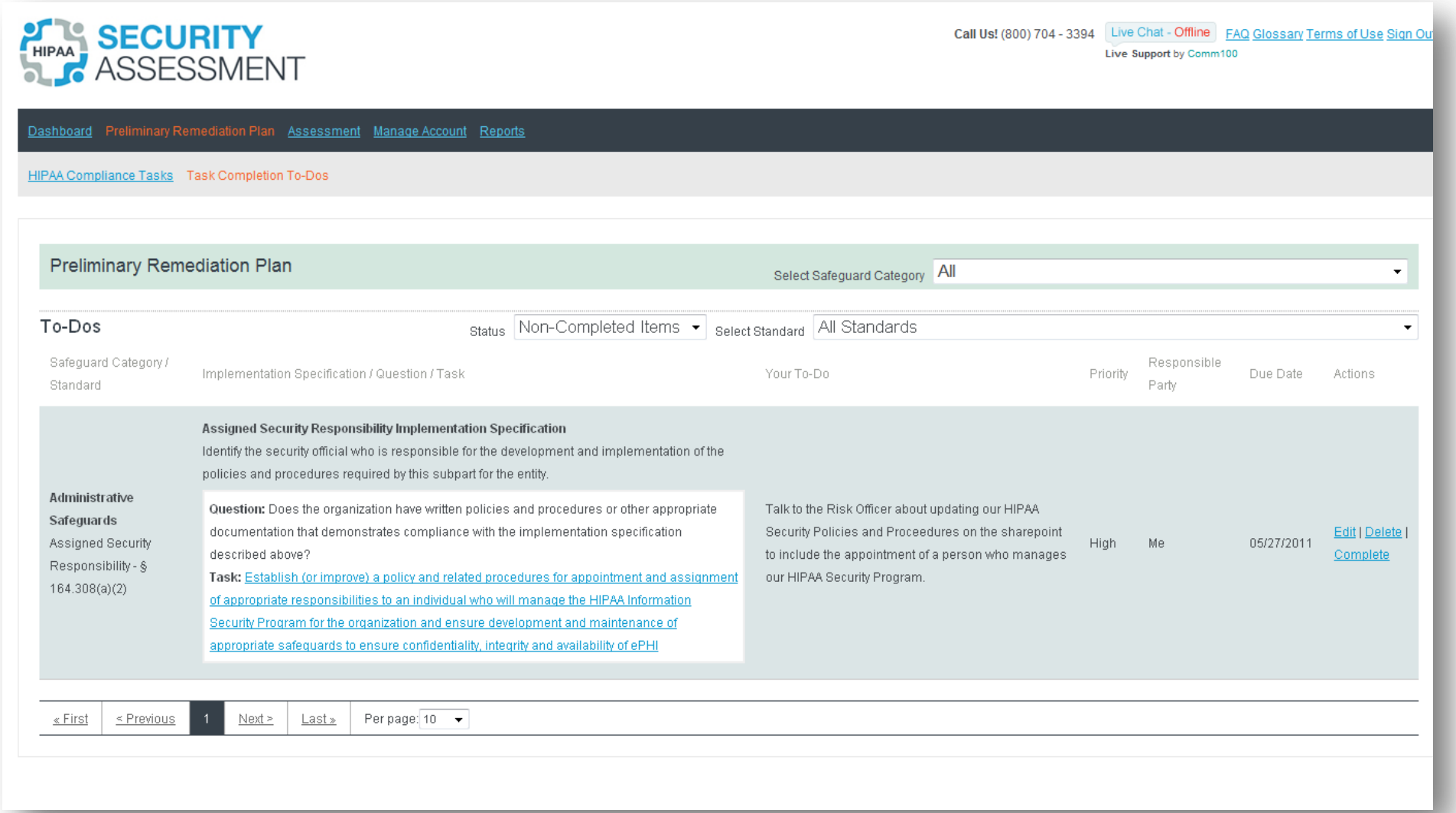


Preliminary Remediation Plan

HIPAA Compliance Tasks

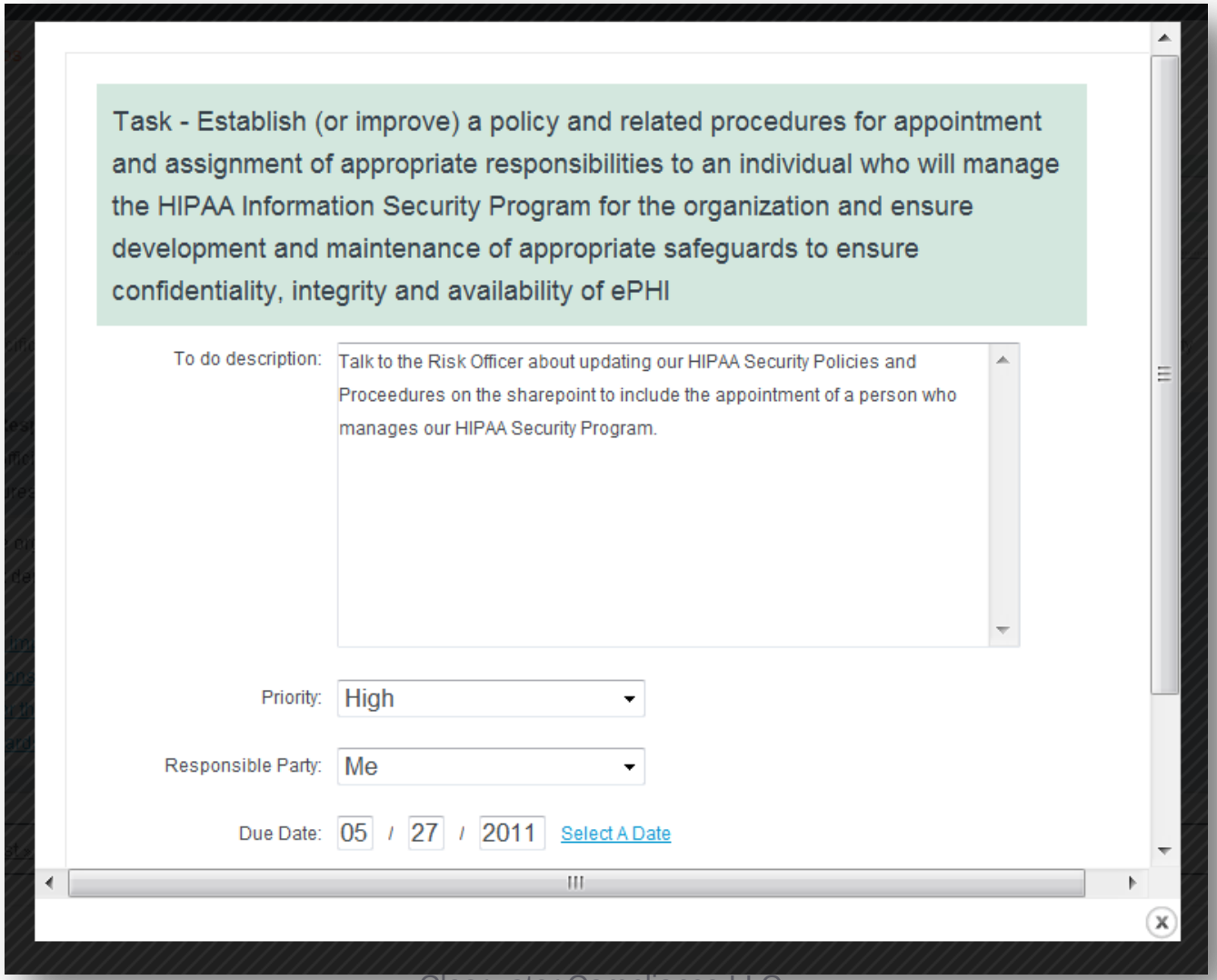


Preliminary Remediation Plan Task Completion To-Dos

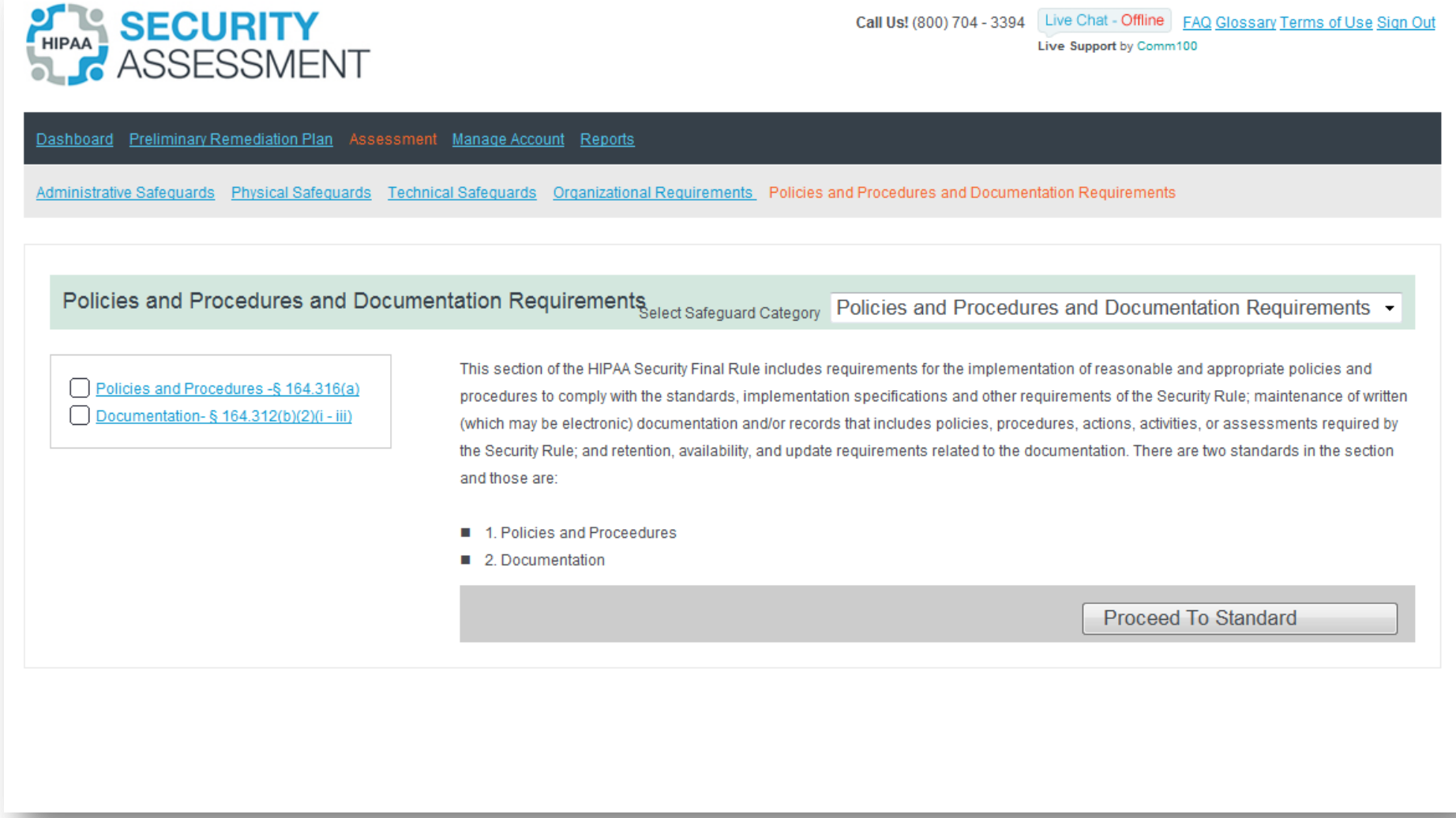


Preliminary Remediation Plan

Add or Edit a To-Do



Assessment Wizard – Safeguard Level



Assessment Wizard – Standard Level