Privacy & Security in Health IT

November 17, 2015

BLUEPRINT HEALTHCARE IT

MeHI MASSACHUSETTS eHEALTH INSTITUTE

at the MassTech Collaborative

Agenda

- Introductions
- Learning Objectives
- Background Information
    - Applicable State and Federal Regulations
    - Consequences of Non-Compliance
- Myths and Facts
- Requirements of HIPAA Security Rule and Meaningful Use
- Common Issues/Trends
- Tools and Resources
- Questions & Answers

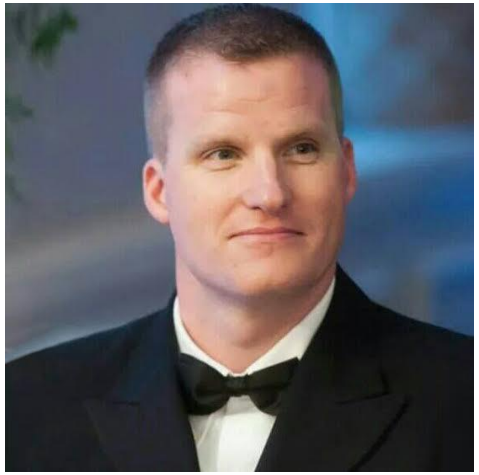
Introductions

BluePrint Healthcare IT

- BluePrint Healthcare IT is a recognized leader in healthcare IT security, privacy, audit readiness, and compliance (S-PAC). Our security services provide a disciplined, standards-based approach to patient and business-centered IT security and privacy risk management.

- BluePrint Healthcare IT is a firm dedicated solely to the healthcare industry, hospitals, health systems, ACOs, payers, and the business associate community. We have been able to anticipate the needs and trends for healthcare IT security, privacy and compliance to build solutions and services that are anticipatory and relevant. We have been leaders, nationally and locally, contributing thought leadership and practical tools for the industry, and contribute to national and regional working groups within HIMSS, HITRUST and eHealth Initiative.

Bio – Ryan Patrick



Ryan Patrick is the Director of BluePrint Healthcare IT’s Security, Privacy, Audit Readiness and Compliance services. With 14 years of experience in all facets of security and information technology for both the public and private sectors, Ryan brings an innovative perspective in protecting information and organizational resources.

Prior to joining BluePrint, Ryan served as the Deputy Chief Information Officer for the New York State Division of Military and Naval Affairs. In that position, he led an effort to prepare for the Defense Information Systems Agency’s (DISA) Command Cyber Readiness Inspection which includes assessing several key areas: the entity’s overall information security program, the classified and unclassified networks and the digital and physical assets used to support them.

Working as a security analyst with organizations such as Metlife and Memorial Sloan-Kettering Cancer Center, Ryan has gained a wealth of experience conducting risk assessments against HIPAA, ISO 27001, NIST 800-53 and PCI-DSS. He currently holds an MBA from Norwich University and the Certified Information Systems Security Professional (CISSP) certification.

Ryan is also a Major in the New York Army National Guard serving as the Chief Information Officer for the 42nd Infantry Division. He is combat veteran of Operation Iraqi Freedom where he received a Bronze Star Medal, Global War on Terrorism Expeditionary Medal and the Global War on Terrorism Service Medal.

Learning Objectives

Learning Objectives

This session is designed to help you:

- Appreciate why Privacy & Security are vital components of Health IT
- Recognize the consequences of non-compliance with applicable state and federal regulations
- Differentiate between Myths and Facts about Security Risk Analysis (SRA) requirements
- Understand the requirements of both the HIPAA Security Rule and the Meaningful Use (MU) Security Risk Analysis objective
- Identify the key components of a thorough Security Risk Analysis
- Implement a Risk Management Process in your organization

Background Information:
State and Federal Regulations

Massachusetts – 201CMR17.00

This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records.

The objectives of this regulation are:

- to ensure the security and confidentiality of customer information in a manner fully consistent with industry standards
- protect against anticipated threats or hazards to the security or integrity of such information
- protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer

- Not only Protected Health Information (PHI)
- Paper or Electronic forms
- Is not a breach unless used in unauthorized manner
- First Initial AND Last Name, PLUS:
  - Social Security Number
  - State-Issued ID (Driver’s License, Photo ID)
  - Account Number (even without PIN)

Massachusetts – 201CMR17.00

Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards.

The comprehensive security program must include:

- Designating one or more employees to maintain the program
- Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information
- Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.

Massachusetts – 201CMR17.00

The comprehensive security program must include (cont):

- Imposing disciplinary measures for violations of the program rules.
- Preventing terminated employees from accessing records containing personal information
- Third-party service providers that are capable of maintaining appropriate security measures to protect such personal information
- Reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers.
- Regular monitoring to ensure that the program to prevent unauthorized access to or unauthorized use of personal information
- Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices
- Mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

Massachusetts 201CMR17.04

The comprehensive information security program must ensure the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:

- User authentication
- Access control
- Encryption (Network)
- System Monitoring
- Encryption (Media)
- Patch Management (Internet-facing)
- Malware
- Education

Massachusetts 201CMR17.00 Breach Notification

“A person who owns or licenses personal information knows or has reason to know of (1) a security breach, or (2) that the personal information of a Massachusetts resident was acquired or used by an unauthorized person or for an unauthorized purpose, that person must notify the Attorney General and the Office of Consumer Affairs and Business Regulation.”

* **Consumer Affairs and Business Regulation website**: http://www.mass.gov/ocabr/data-privacy-and-security/data/requirements-for-security-breach-notifications.html

The notifications to the Office of Consumer Affairs and Business Regulation and to the Attorney General must include:

- A detailed description of the nature and circumstances of the breach of security or unauthorized acquisition or use of personal information;
- The number of Massachusetts residents affected as of the time of notification;
- The steps already taken relative to the incident;
- Any steps intended to be taken relative to the incident subsequent to notification; and
- Information regarding whether law enforcement is engaged investigating the incident.

Federal Law/Regulations

Applicable Federal Law and/or Regulations include:

- HIPAA
- HITECH
- OMNIBUS

***Systems and controls should comply with most stringent requirements**

HIPAA & HITECH Background

HITECH (Health Information Technology for Economic and Clinical Health): enacted on February 17, 2009.

- Part of the **American Recovery & Reinvestment Act (ARRA)**
- Revised **HIPAA** (Health Insurance Portability and Accountability Act) rule: tougher provisions for security, privacy and enforcement.
- Increased maximum penalties:
  - $50,000 per incident
  - $1.5M for the year (willful neglect concept)
- Reporting requirements for security breaches
  - Media outlets, US Department of Health and Human Services, victims
- Ability for state Attorney General to bring legal action against physicians and hospitals for non-compliance
- Individual Liability for criminal violations

Violations = Penalties

Violation Category	Per Violation	Maximum Penalty Per Year
Violation was not known and the organization would not have known by exercising reasonable diligence.	$100 - $50,000	$1.5 M
Violations due to reasonable cause but not willful neglect.	$1,000 - $50,000	$1.5 M
Violation due to willful neglect but corrected within 30 days of discovery of the violation.	$10,000 - $50,000	$1.5 M
Violation due to willful neglect and not corrected within 30 days of discovery.	$50,000	$1.5 M

HITECH – New Provisions

- Business Associates and subcontractors are now subject to HIPAA requirements (“Chain of Trust”)
- Restrictions on Research, Marketing, Fundraising, Sale of patient information
- Increased patient rights to restrict disclosure of PHI
- Business Associate Agreements must be revised to include language that covers HITECH & OMNIBUS
- Length of time information is considered PHI
- Accounting of Disclosures to include TPO (Treatment, Payment and Operations)

OMNIBUS – New Provisions

- Expanded Business Associate (BA) definition
- Third-Party Risk Assessments
- Strengthened “harm” provision
  - Assumption of harm unless proven otherwise
- Genetic Information Nondiscrimination Act (GINA)
  - Genetic information is protected under the HIPAA Privacy Rule

Background Information: Consequences of Non-Compliance

The Hard Truth!

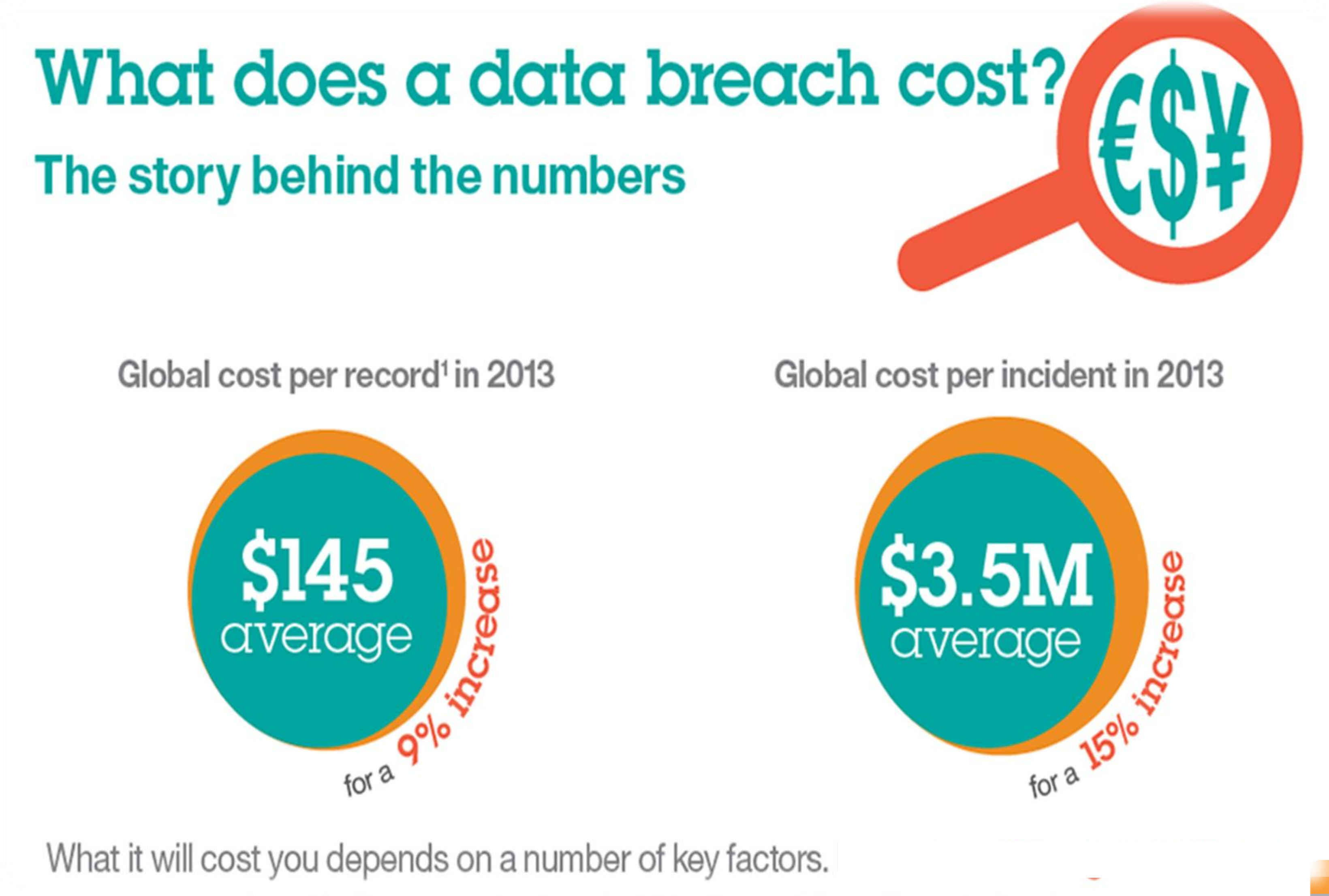
You may be wondering…

Why are you telling me all of this?

What does this mean to me?

Why are we here?

Ponemon Institute *2014 Cost of Data Breach Study: Global Analysis*



What does a data breach cost?

The story behind the numbers

Global cost per record[1] in 2013

$145 average

for a 9% increase

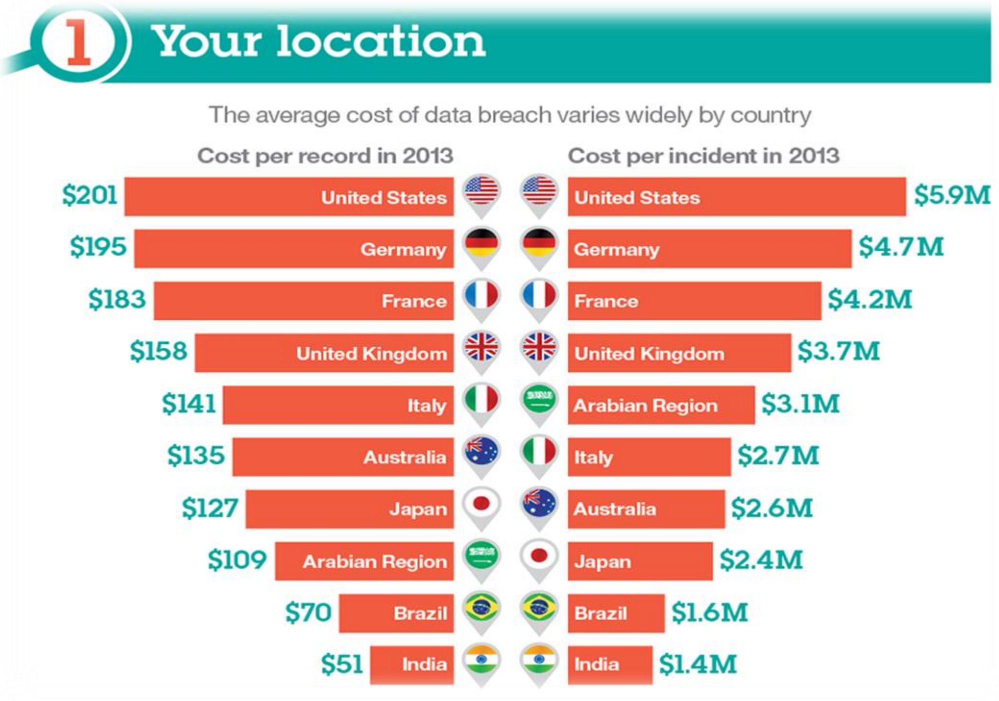
Global cost per incident in 2013

$3.5M average

for a 15% increase

What it will cost you depends on a number of key factors.

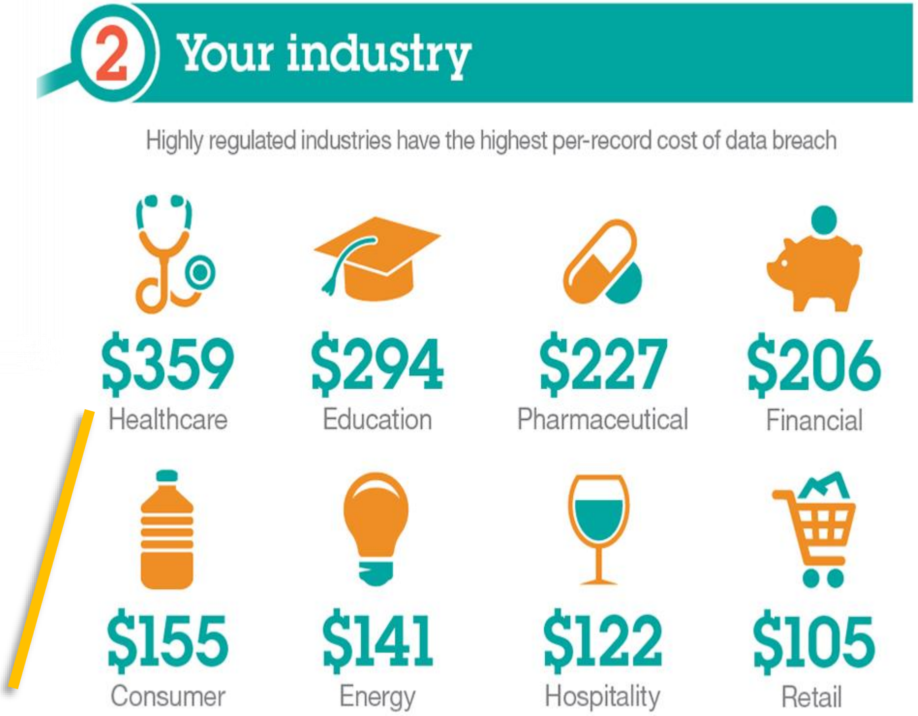
Ponemon Institute *2014 Cost of Data Breach Study: Global Analysis*



1 Your location

The average cost of data breach varies widely by country

Cost per record in 2013		Cost per incident in 2013	
$201	United States	United States	$5.9M
$195	Germany	Germany	$4.7M
$183	France	France	$4.2M
$158	United Kingdom	United Kingdom	$3.7M
$141	Italy	Arabian Region	$3.1M
$135	Australia	Italy	$2.7M
$127	Japan	Australia	$2.6M
$109	Arabian Region	Japan	$2.4M
$70	Brazil	Brazil	$1.6M
$51	India	India	$1.4M



2 Your industry

Highly regulated industries have the highest per-record cost of data breach

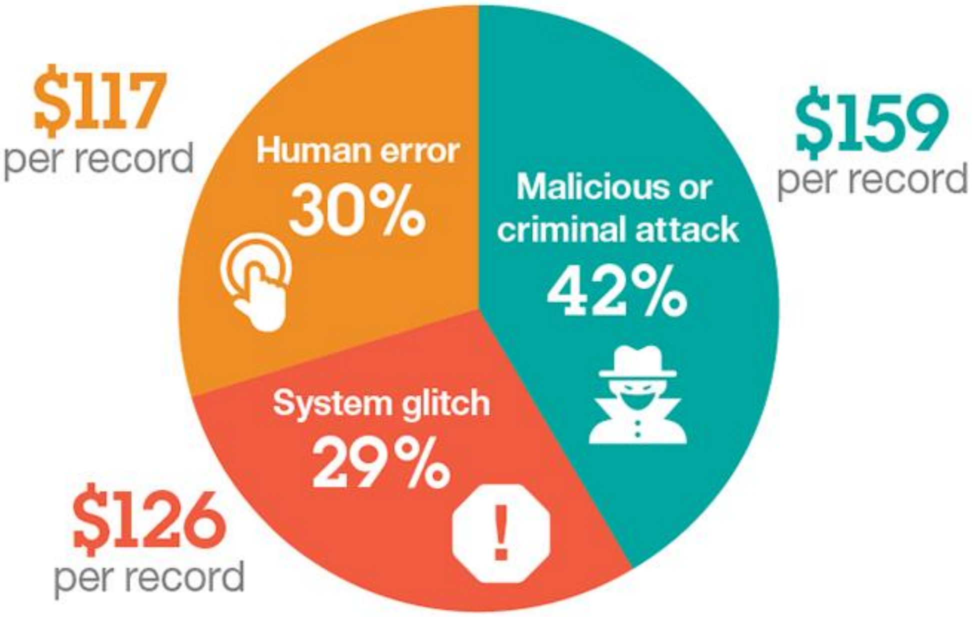
$359 Healthcare	$294 Education	$227 Pharmaceutical	$206 Financial
$155 Consumer	$141 Energy	$122 Hospitality	$105 Retail

THIS is why we are here…

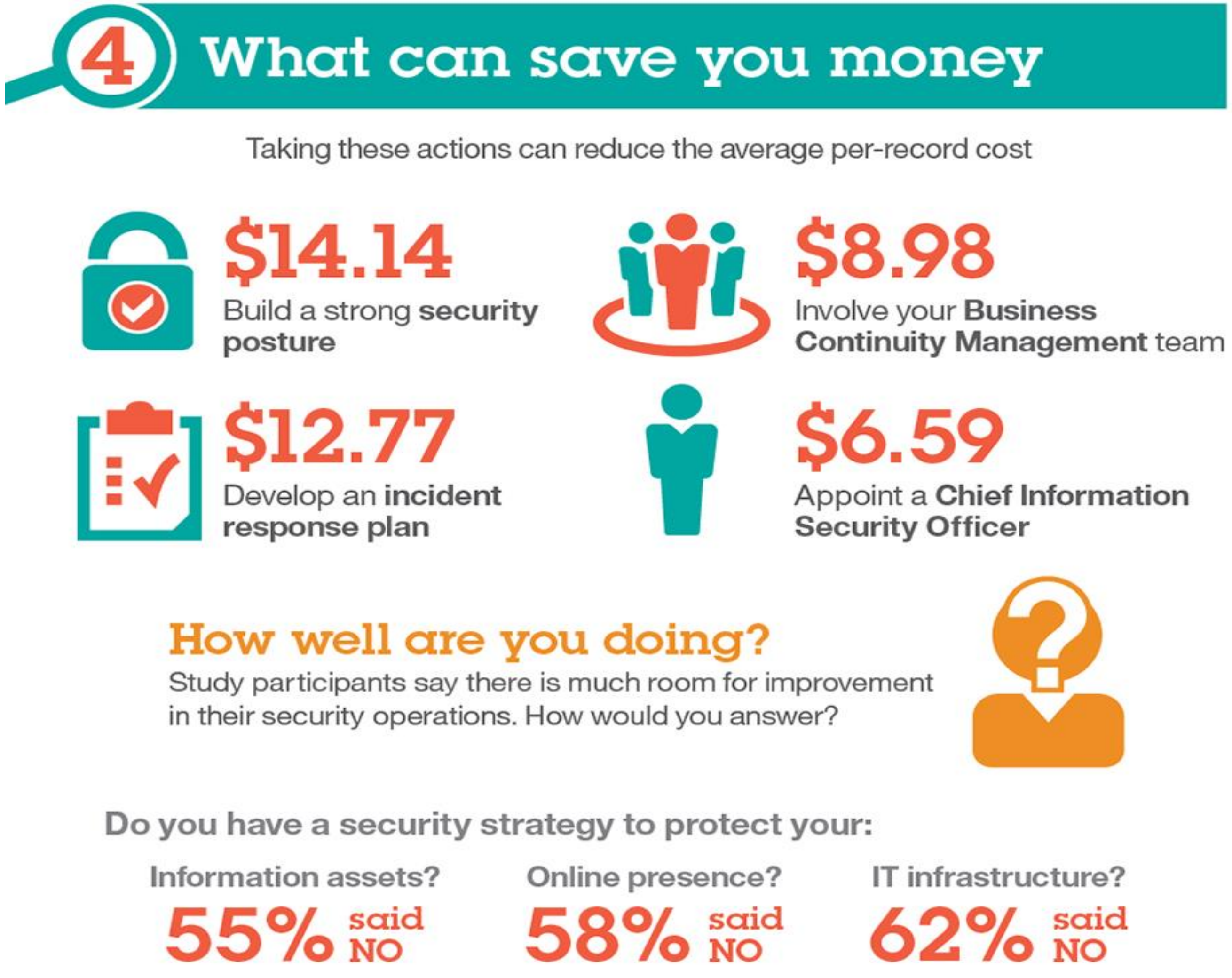
Ponemon Institute *2014 Cost of Data Breach Study: Global Analysis*

3 The type of attack

Malicious or criminal attacks are the leading root cause of a data breach…
and result in the highest cost per record



Ponemon Institute *2014 Cost of Data Breach Study: Global Analysis*



4 What can save you money

Taking these actions can reduce the average per-record cost

$14.14
Build a strong **security posture**

$8.98
Involve your **Business Continuity Management** team

$12.77
Develop an **incident response plan**

$6.59
Appoint a **Chief Information Security Officer**

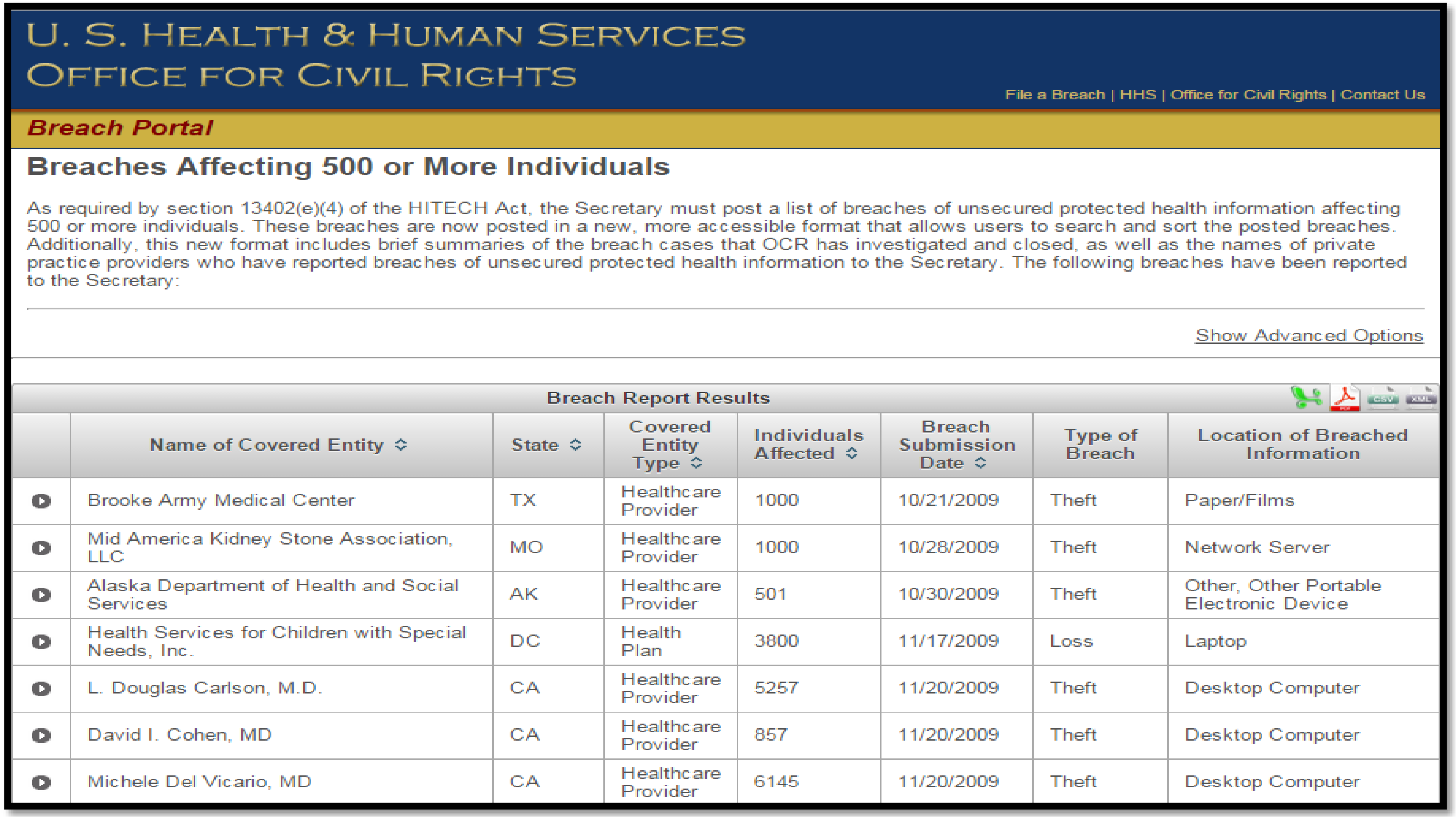
How well are you doing?

Study participants say there is much room for improvement in their security operations. How would you answer?

Do you have a security strategy to protect your:

Information assets?	Online presence?	IT infrastructure?
55% said NO	58% said NO	62% said NO

HHS Breach Notification Site



U. S. HEALTH & HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

File a Breach | HHS | Office for Civil Rights | Contact Us

Breach Portal

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:

Show Advanced Options

Breach Report Results

	Name of Covered Entity ⇕	State ⇕	Covered Entity Type ⇕	Individuals Affected ⇕	Breach Submission Date ⇕	Type of Breach	Location of Breached Information
▶	Brooke Army Medical Center	TX	Healthcare Provider	1000	10/21/2009	Theft	Paper/Films
▶	Mid America Kidney Stone Association, LLC	MO	Healthcare Provider	1000	10/28/2009	Theft	Network Server
▶	Alaska Department of Health and Social Services	AK	Healthcare Provider	501	10/30/2009	Theft	Other, Other Portable Electronic Device
▶	Health Services for Children with Special Needs, Inc.	DC	Health Plan	3800	11/17/2009	Loss	Laptop
▶	L. Douglas Carlson, M.D.	CA	Healthcare Provider	5257	11/20/2009	Theft	Desktop Computer
▶	David I. Cohen, MD	CA	Healthcare Provider	857	11/20/2009	Theft	Desktop Computer
▶	Michele Del Vicario, MD	CA	Healthcare Provider	6145	11/20/2009	Theft	Desktop Computer

There have been *1,366* reported breaches of 500 records or more since October 21, 2009. *224* since March 2015 alone…

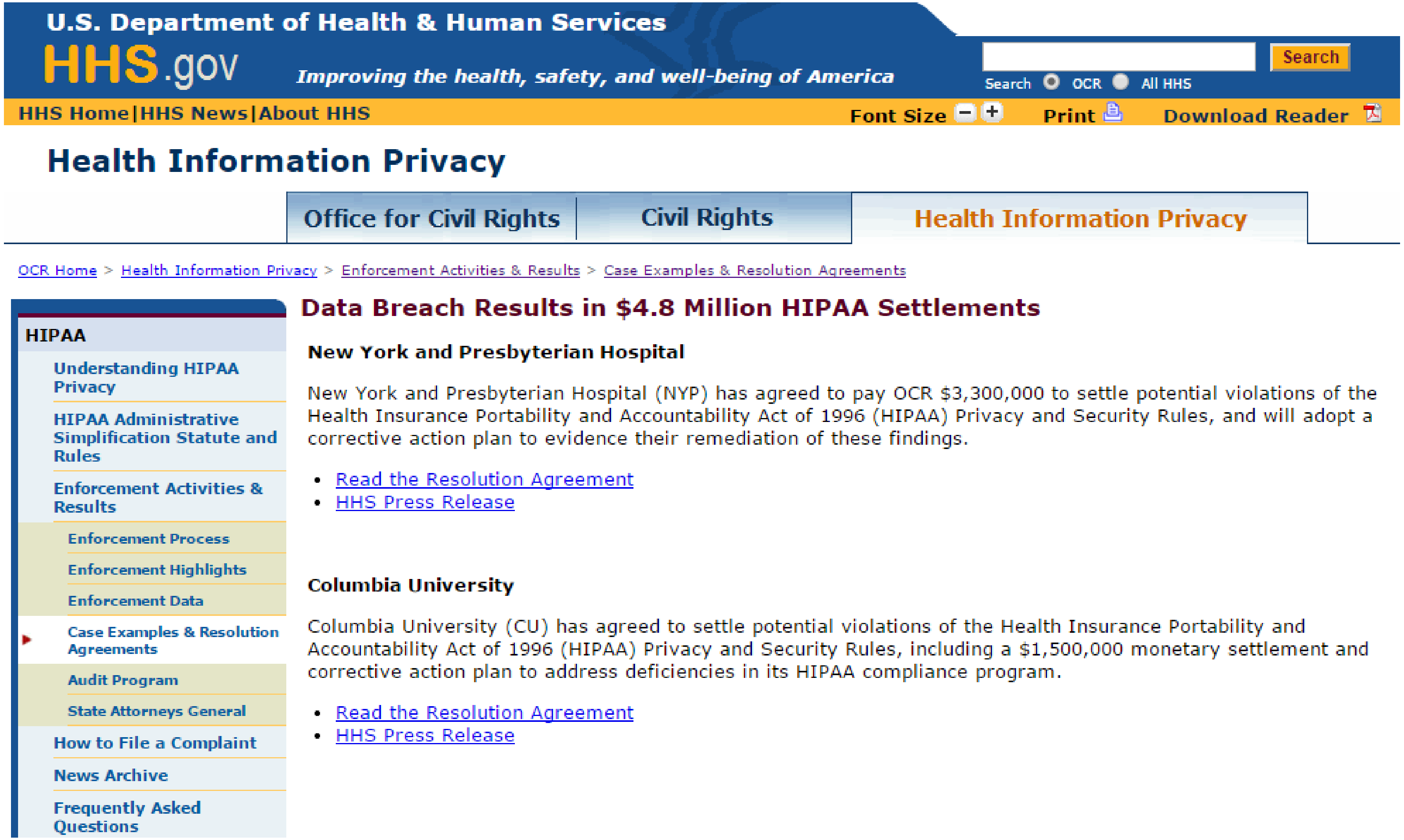
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

BLUEPRINT HEALTHCARE IT

MeHI MASSACHUSETTS eHEALTH INSTITUTE

at the MassTech Collaborative

Settlements Reached with HHS



U.S. Department of Health & Human Services
HHS.gov
Improving the health, safety, and well-being of America
Search
Search ● OCR ○ All HHS
HHS Home | HHS News | About HHS
Font Size − +
Print
Download Reader

Health Information Privacy

Office for Civil Rights
Civil Rights
Health Information Privacy

OCR Home > Health Information Privacy > Enforcement Activities & Results > Case Examples & Resolution Agreements

HIPAA
Understanding HIPAA Privacy
HIPAA Administrative Simplification Statute and Rules
Enforcement Activities & Results
Enforcement Process
Enforcement Highlights
Enforcement Data
Case Examples & Resolution Agreements
Audit Program
State Attorneys General
How to File a Complaint
News Archive
Frequently Asked Questions

Data Breach Results in $4.8 Million HIPAA Settlements

New York and Presbyterian Hospital

New York and Presbyterian Hospital (NYP) has agreed to pay OCR $3,300,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, and will adopt a corrective action plan to evidence their remediation of these findings.

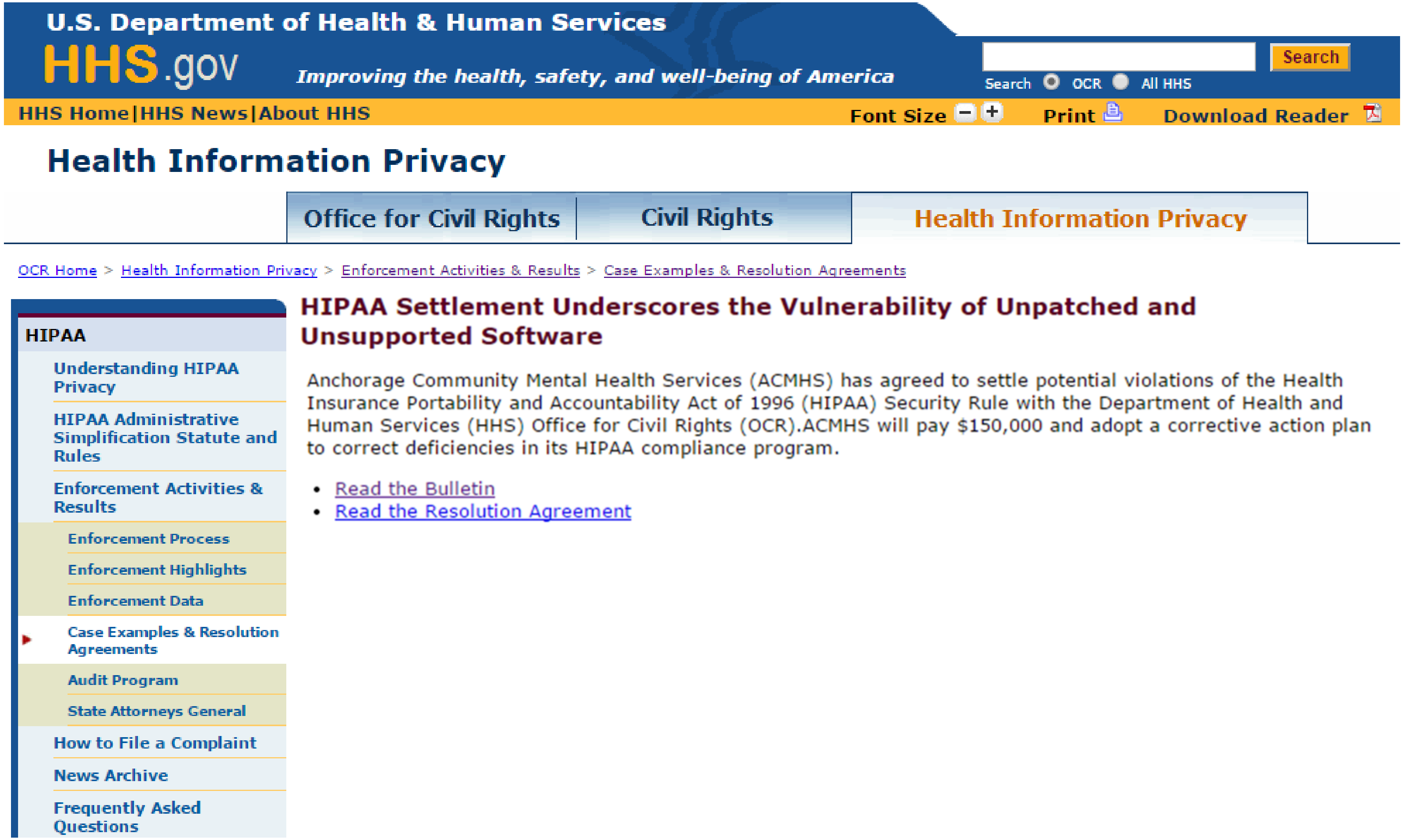
- Read the Resolution Agreement
- HHS Press Release

Columbia University

Columbia University (CU) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, including a $1,500,000 monetary settlement and corrective action plan to address deficiencies in its HIPAA compliance program.

- Read the Resolution Agreement
- HHS Press Release

Settlements Reached with HHS


U.S. Department of Health & Human Services
HHS.gov
Improving the health, safety, and well-being of America
Search
Search ○ OCR ○ All HHS
HHS Home | HHS News | About HHS
Font Size − +
Print
Download Reader
Office for Civil Rights
Civil Rights
Health Information Privacy
HIPAA
Understanding HIPAA Privacy
HIPAA Administrative Simplification Statute and Rules
Enforcement Activities & Results
Enforcement Process
Enforcement Highlights
Enforcement Data
Case Examples & Resolution Agreements
Audit Program
State Attorneys General
How to File a Complaint
News Archive
Frequently Asked Questions

Health Information Privacy

OCR Home > Health Information Privacy > Enforcement Activities & Results > Case Examples & Resolution Agreements

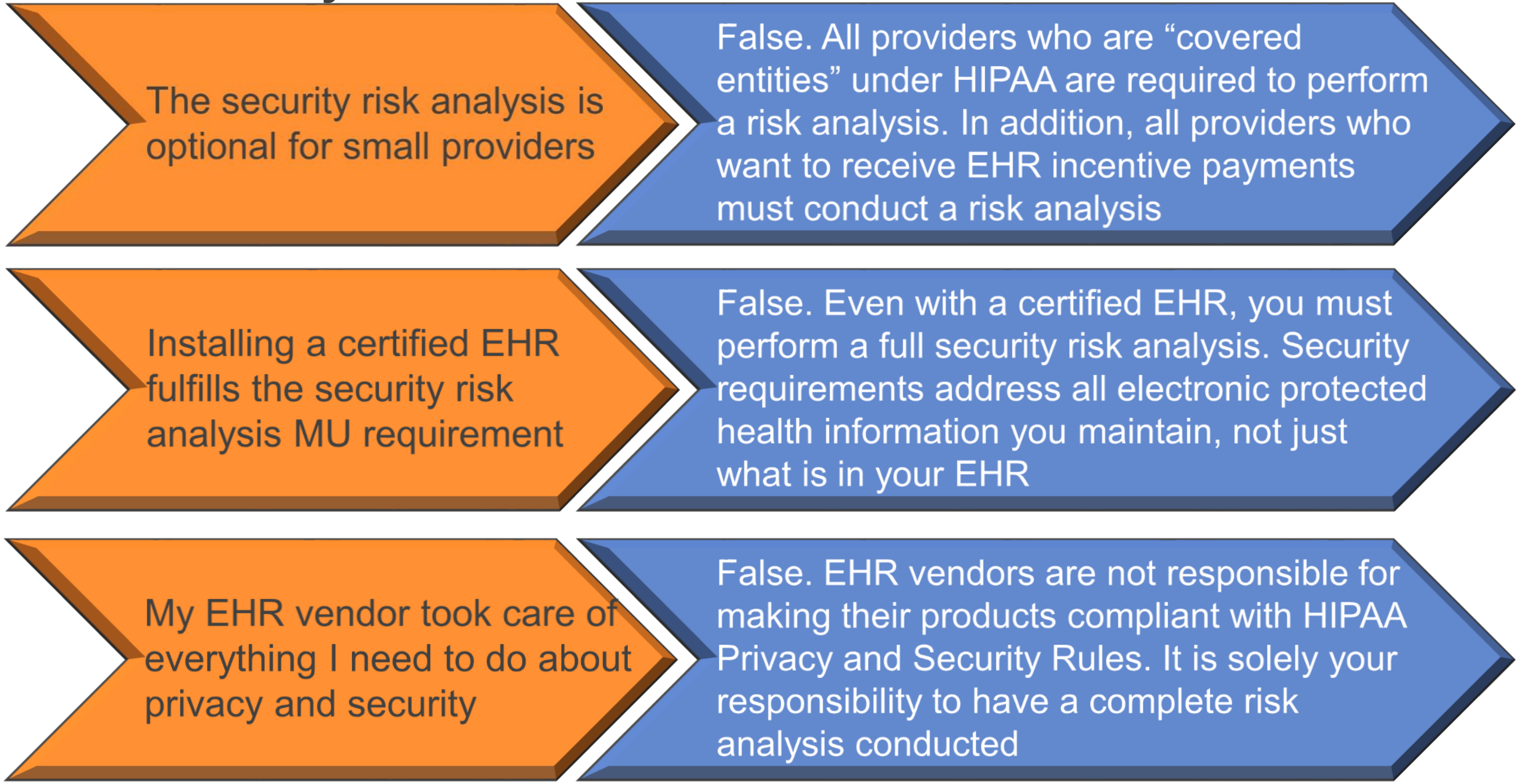
HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software

Anchorage Community Mental Health Services (ACMHS) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule with the Department of Health and Human Services (HHS) Office for Civil Rights (OCR).ACMHS will pay $150,000 and adopt a corrective action plan to correct deficiencies in its HIPAA compliance program.

- Read the Bulletin
- Read the Resolution Agreement

Privacy & Security Rule: Myths and Facts

10 Myths of Security Rule and Meaningful Use



Myth	Fact
The security risk analysis is optional for small providers	False. All providers who are “covered entities” under HIPAA are required to perform a risk analysis. In addition, all providers who want to receive EHR incentive payments must conduct a risk analysis
Installing a certified EHR fulfills the security risk analysis MU requirement	False. Even with a certified EHR, you must perform a full security risk analysis. Security requirements address all electronic protected health information you maintain, not just what is in your EHR
My EHR vendor took care of everything I need to do about privacy and security	False. EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. It is solely your responsibility to have a complete risk analysis conducted

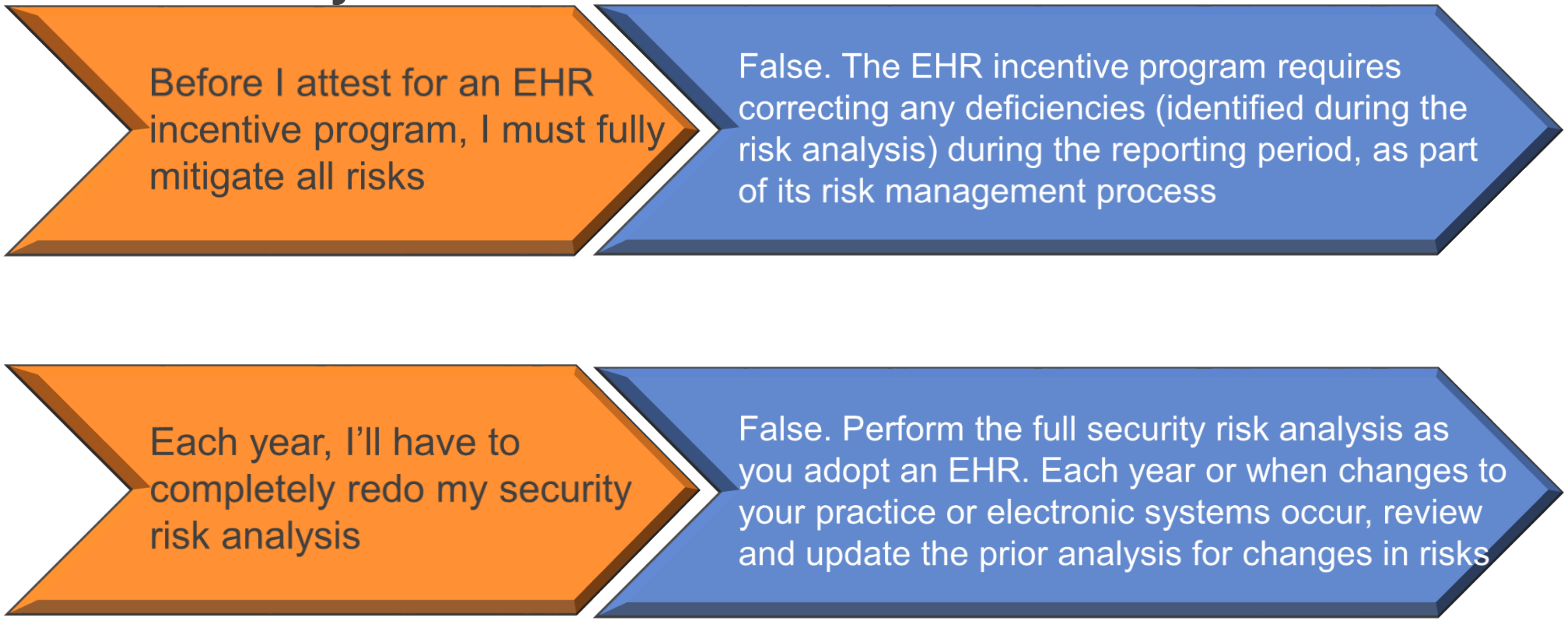
10 Myths of Security Rule and Meaningful Use

Myth	Fact
I have to outsource the security risk analysis	False. It is possible for small practices to do risk analysis themselves. However, doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge.
A checklist will suffice for the risk analysis requirement	False. Checklists can be useful tools, especially when starting a risk analysis, but they fall short of performing a systematic security risk analysis or documenting that one has been performed.
There is a specific risk analysis method that I must follow	False. A risk analysis can be performed in countless ways. OCR has issued Guidance on Risk Analysis Requirements of the Security Rule.

10 Myths of Security Rule and Meaningful Use

Myth	Fact
My security risk analysis only needs to look at my EHR	False. Review all electronic devices that store, capture, or modify electronic protected health information. Include your EHR hardware and software and devices that can access your EHR data (e.g., your tablet, your mobile phone, etc)
I only need to do a risk analysis once	False. To comply with HIPAA, you must continue to review, correct or modify, and update security protections.

10 Myths of Security Rule and Meaningful Use



Myth	Fact
Before I attest for an EHR incentive program, I must fully mitigate all risks	False. The EHR incentive program requires correcting any deficiencies (identified during the risk analysis) during the reporting period, as part of its risk management process
Each year, I'll have to completely redo my security risk analysis	False. Perform the full security risk analysis as you adopt an EHR. Each year or when changes to your practice or electronic systems occur, review and update the prior analysis for changes in risks

Requirements of HIPAA Security Rule and Meaningful Use

HIPAA – Security Goal

Privacy and security is the responsibility of physicians and their staff.

HIPAA Security Risk Analysis – General Categories

PHYSICAL SAFEGUARDS

- Facility Access Control
- Workstation Use
- Workstation Security
- Device and Media Controls

ADMINISTRATIVE SAFEGUARDS

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation

TECHNICAL SAFEGUARDS

- Access Control
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS

- Written policies and procedures to assure HIPAA security compliance
- Documentation of security measures

ORGANIZATIONAL REQUIREMENTS

- Business Associate Contracts and Other Arrangements
- Requirements for Group Health Plans

HIPAA Security Rule – Risk Management

Under the Administrative safeguards, a covered entity must:

- Establish and maintain a security management **process**
- Implement policies and procedures to prevent, detect, contain, and correct security violations
- Implementation specifications:

  ✓ 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.

  ✓ Risk management (Required): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level

HIPAA Security Rule – Risk Analysis Guidance

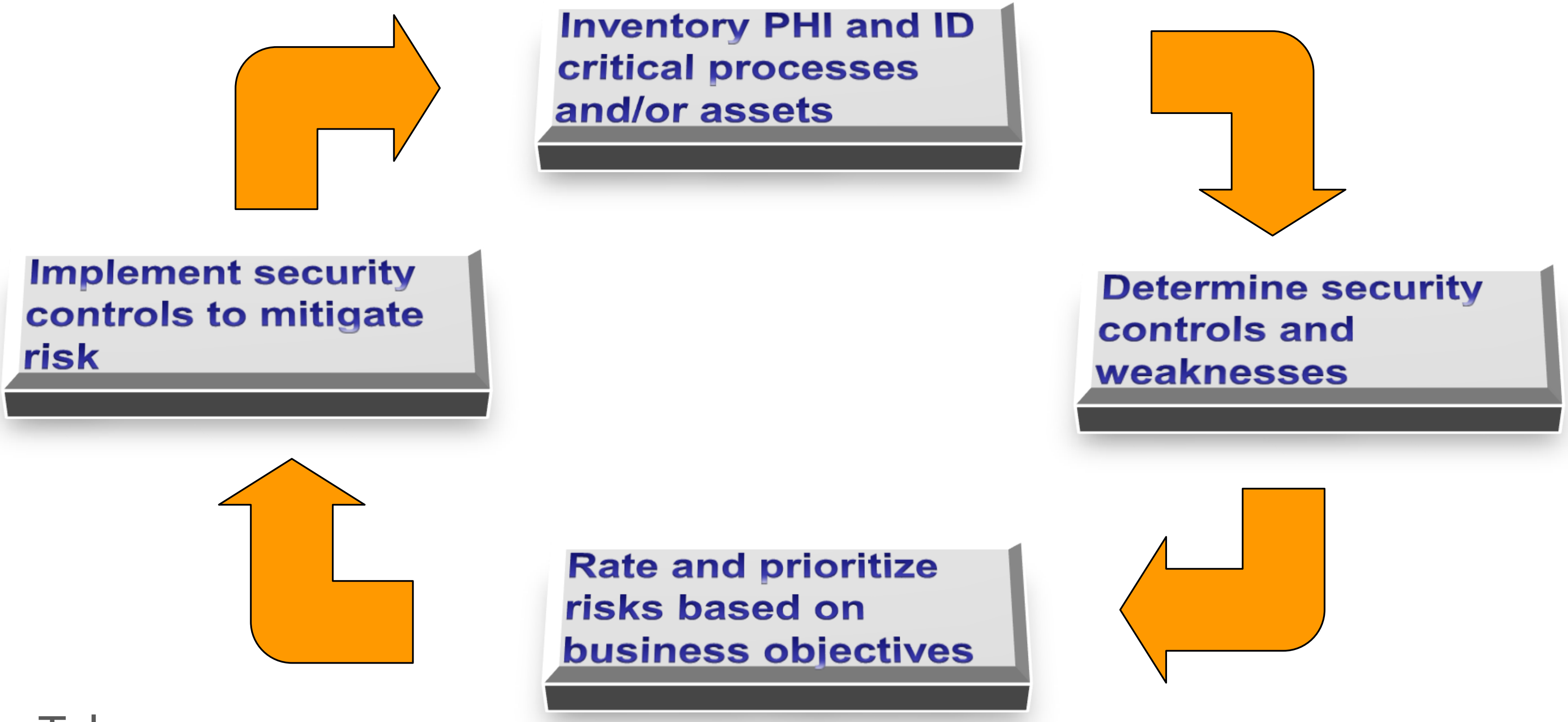
Health and Human Services issued guidance for conducting the required risk analysis:

- Scope
- Data Collection
- Identify and document threats and vulnerabilities
- Assess current security measures
- Determine likelihood of threat occurrence
- Determine potential impact of threat occurrence
- Determine level of risk
- Finalize documentation
- Periodic review and updates to the risk analysis

Identify
Assess
Manage
Safeguard

*http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidance.pdf

HIPAA Security Rule – Risk Management Process



Inventory PHI and ID critical processes and/or assets

Determine security controls and weaknesses

Rate and prioritize risks based on business objectives

Implement security controls to mitigate risk

Takeaways

- Know how and where your organization is at risk and determine the appropriate strategy
- Implement continuous risk management process
- The operative word is **process**

HIPAA Security Rule – Risk Analysis Guidance

Health and Human Services issued guidance for conducting the required risk analysis:

Identify
Assess
Manage
Safeguard

- Scope
- Data Collection
- Identify and document threats and vulnerabilities
- Assess current security measures
- Determine likelihood of threat occurrence
- Determine potential impact of threat occurrence
- Determine level of risk
- Finalize documentation
- Periodic review and updates to the risk analysis

*http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidance.pdf

HIPAA Security Rule and Meaningful Use

- For the Medicare and Medicaid EHR Incentive Programs, providers have to demonstrate that they are meaningfully using their EHRs by meeting thresholds for a number of objectives.
- CMS recently released a Final Rule that defines a revised set of Meaningful Use objectives and measures.
- All EPs attest to Modified Stage 2 objectives, with accommodations for Stage 1 EPs in 2015 and 2016.

- Meaningful Use Objectives – Modified Stage 2
  1. Protect Patient Health Information – Security Risk Analysis
  2. Clinical Decision Support (CDS)
  3. Computerized Provider Order Entry (CPOE)
  4. Electronic Prescribing (eRx)
  5. Health Information Exchange (HIE) – *previously known as "Summary of Care"*
  6. Patient Specific Education
  7. Medication Reconciliation
  8. Patient Electronic Access (Patient Portal)
  9. Secure Electronic Messaging (Eligible Professionals only)
  10. Public Health and Clinical Data Registry Reporting
      a. Immunization Registry Reporting
      b. Syndromic Surveillance Reporting
      c. Specialized Registry Reporting
      d. Reportable Lab Results Reporting (Eligible Hospitals only)

Meaningful Use – Security Risk Analysis Objective

From the CMS Final Rule published October 16, 2015

Objective 1: Protect Patient Health Information

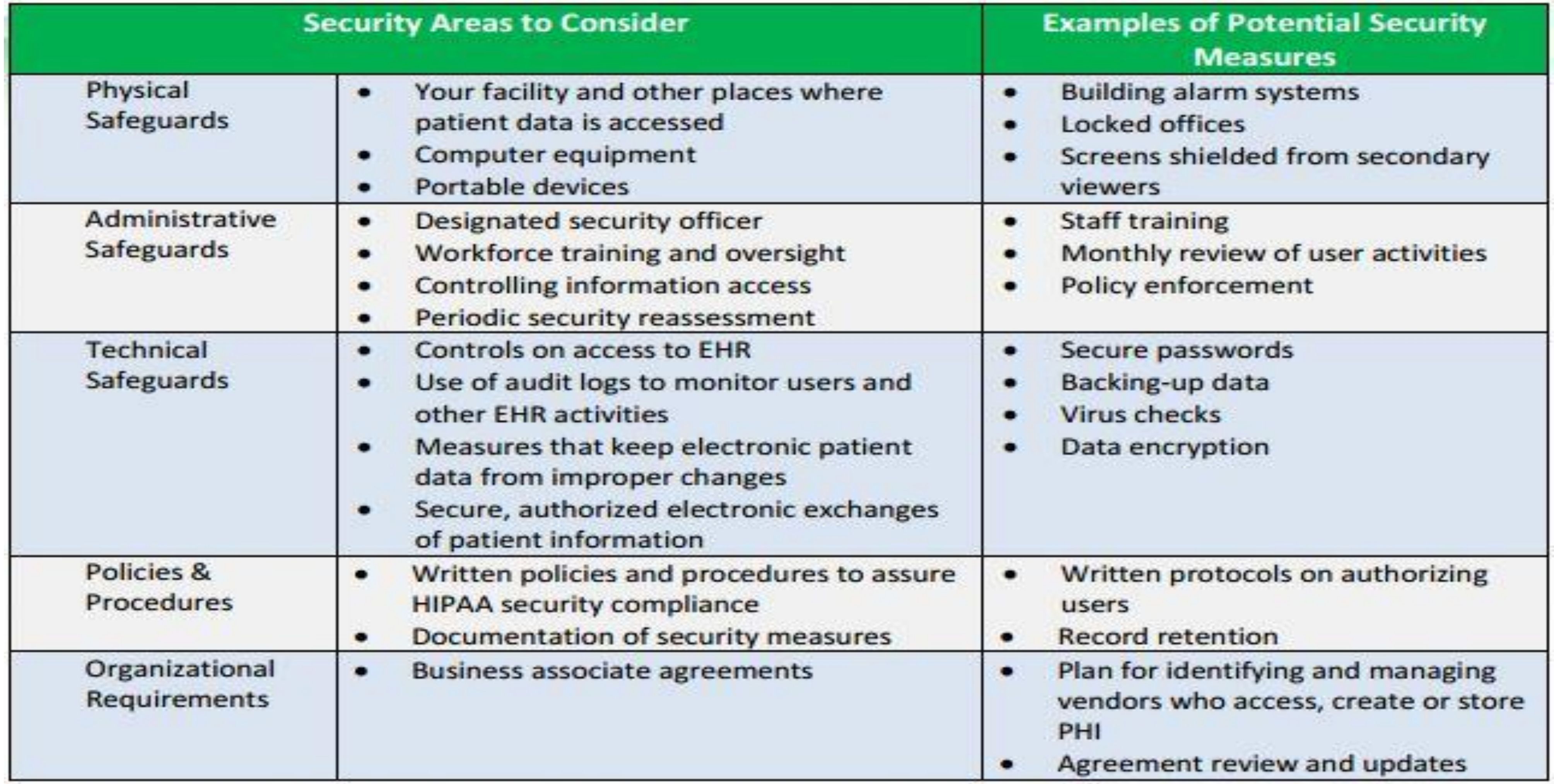
Objective:
Protect electronic health information created or maintained by the CEHRT through the implementation of appropriate technical capabilities.

Measure:
Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI created or maintained by CEHRT in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the EP, eligible hospital, or CAH's risk management process.

Exclusion: None

Note: A review must be conducted for each EHR reporting period and any security updates and deficiencies that are identified should be included in the provider's risk management process and implemented or corrected as dictated by that process.

MU Security Risk Analysis – Key Components



Security Areas to Consider		Examples of Potential Security Measures
Physical Safeguards	• Your facility and other places where patient data is accessed • Computer equipment • Portable devices	• Building alarm systems • Locked offices • Screens shielded from secondary viewers
Administrative Safeguards	• Designated security officer • Workforce training and oversight • Controlling information access • Periodic security reassessment	• Staff training • Monthly review of user activities • Policy enforcement
Technical Safeguards	• Controls on access to EHR • Use of audit logs to monitor users and other EHR activities • Measures that keep electronic patient data from improper changes • Secure, authorized electronic exchanges of patient information	• Secure passwords • Backing-up data • Virus checks • Data encryption
Policies & Procedures	• Written policies and procedures to assure HIPAA security compliance • Documentation of security measures	• Written protocols on authorizing users • Record retention
Organizational Requirements	• Business associate agreements	• Plan for identifying and managing vendors who access, create or store PHI • Agreement review and updates

Source: https://www.cms.gov/regulations-and-guidance/legislation/ehrincentiveprograms/downloads/securityriskassessment_factsheet_updated20131122.pdf

Common Issues or Trends BluePrint sees…

We conduct a Security Risk Analysis for variety of healthcare organizations:

- Large multi-hospital systems
- Business associates
- ACOs
- Community practices

Three most commons issues or trends:

- Ineffective security awareness training
- Organizational policies and procedures
- System configurations and maintenance

Tools and Resources

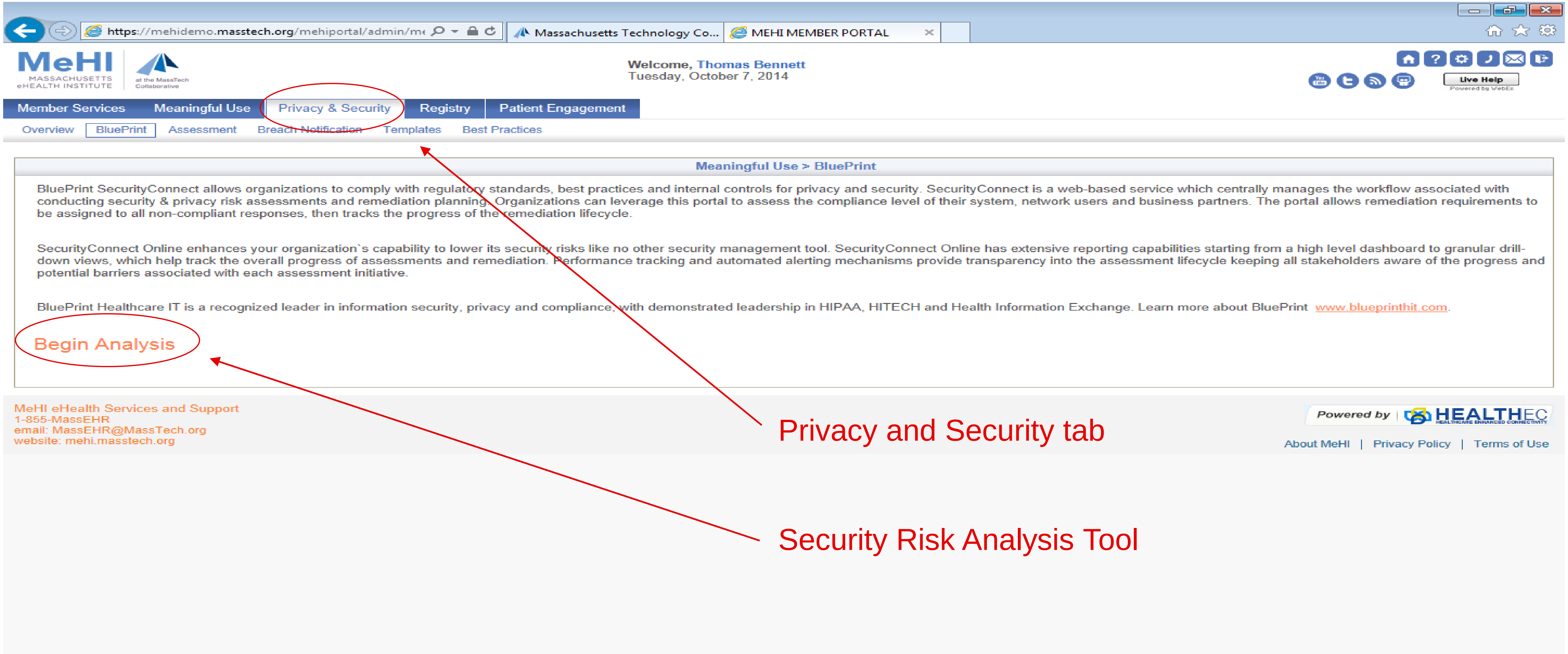
Helpful Links

- CMS Security Risk Assessment Tip Sheet
- ONC Privacy & Security Guide
- ONC Security Risk Analysis Video
- ONC Privacy & Security Webpage
- CMS Final Rule: Stage 3 and Modifications to MU for 2015-2017
- HIPAA Security Rule
- HIPAA Privacy Rule
- HIPAA Risk Analysis Guidance

MeHI Member Portal

MeHI Member Portal Features and Tools
▪ Meaningful Use Gap Analysis
▪ Privacy and Security / BluePrint: Secure™
▪ Patient Engagement / Consumer eHealth Readiness Tool™
▪ Registration and Attestation
▪ Data collection and other forms
▪ Policy and government regulations guidance
▪ CMS-qualified Registry
▪ Document storage and audit preparation
▪ Secure messaging
▪ Live Help
▪ Frequently Asked Questions (FAQs)
▪ Administrative tools

MeHI Member Portal



Welcome, Thomas Bennett
Tuesday, October 7, 2014

Meaningful Use > BluePrint

BluePrint SecurityConnect allows organizations to comply with regulatory standards, best practices and internal controls for privacy and security. SecurityConnect is a web-based service which centrally manages the workflow associated with conducting security & privacy risk assessments and remediation planning. Organizations can leverage this portal to assess the compliance level of their system, network users and business partners. The portal allows remediation requirements to be assigned to all non-compliant responses, then tracks the progress of the remediation lifecycle.

SecurityConnect Online enhances your organization`s capability to lower its security risks like no other security management tool. SecurityConnect Online has extensive reporting capabilities starting from a high level dashboard to granular drill-down views, which help track the overall progress of assessments and remediation. Performance tracking and automated alerting mechanisms provide transparency into the assessment lifecycle keeping all stakeholders aware of the progress and potential barriers associated with each assessment initiative.

BluePrint Healthcare IT is a recognized leader in information security, privacy and compliance, with demonstrated leadership in HIPAA, HITECH and Health Information Exchange. Learn more about BluePrint www.blueprinthit.com.

Begin Analysis

MeHI eHealth Services and Support
1-855-MassEHR
email: MassEHR@MassTech.org
website: mehi.masstech.org

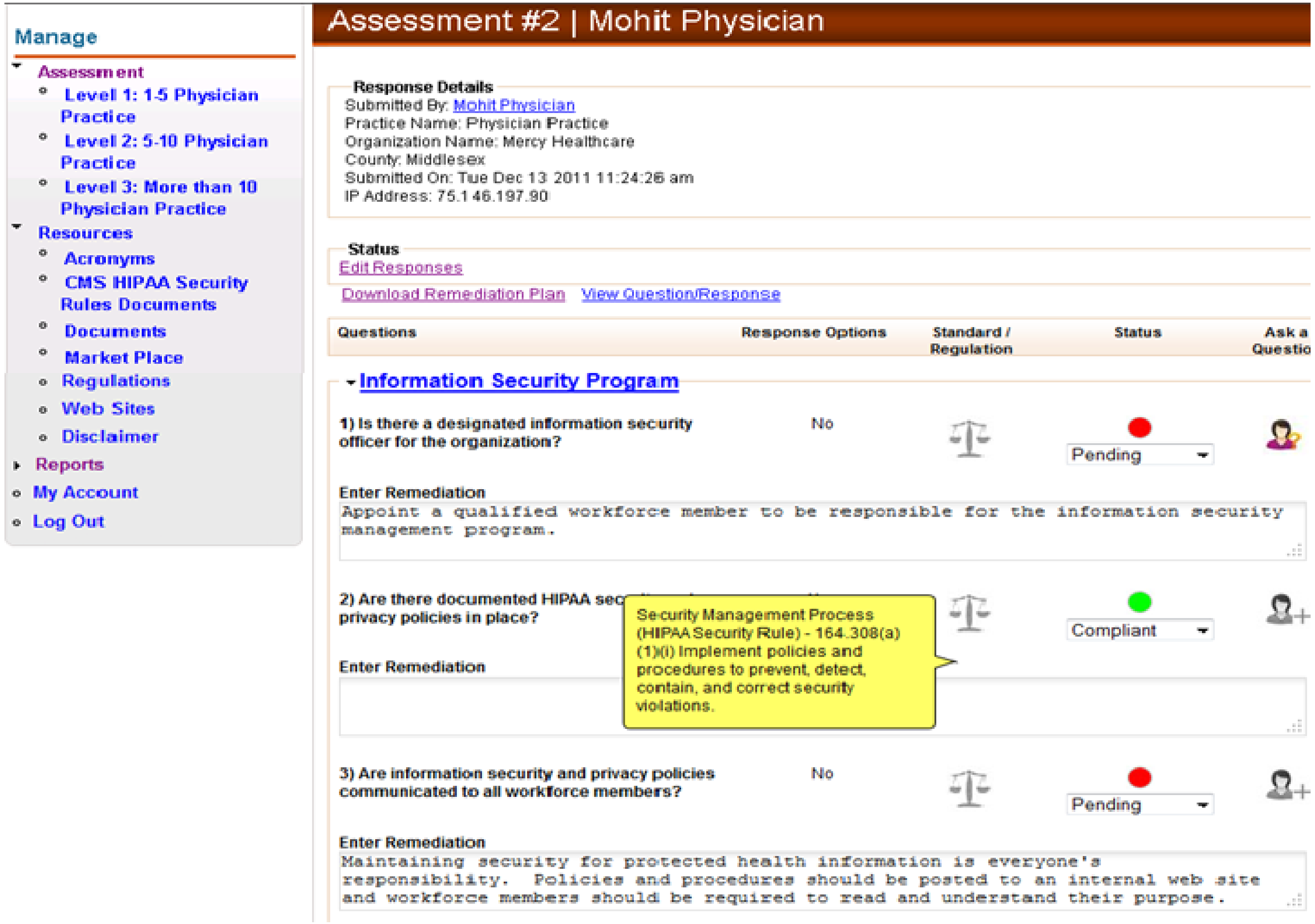
Powered by HEALTHEC

About MeHI | Privacy Policy | Terms of Use

Privacy and Security tab

Security Risk Analysis Tool

BluePrint SecurityConnect - Assessment


Manage
Assessment
Level 1: 1-5 Physician Practice
Level 2: 5-10 Physician Practice
Level 3: More than 10 Physician Practice
Resources
Acronyms
CMS HIPAA Security Rules Documents
Documents
Market Place
Regulations
Web Sites
Disclaimer
Reports
My Account
Log Out

Assessment #2 | Mohit Physician

Response Details

Submitted By: Mohit Physician
Practice Name: Physician Practice
Organization Name: Mercy Healthcare
County: Middlesex
Submitted On: Tue Dec 13 2011 11:24:26 am
IP Address: 75.146.197.90

Status

Edit Responses

Download Remediation Plan   View Question/Response

Questions	Response Options	Standard / Regulation	Status	Ask a Questio
Information Security Program				
1) Is there a designated information security officer for the organization?	No		🔴 Pending	
2) Are there documented HIPAA sec... privacy policies in place?			🟢 Compliant	
3) Are information security and privacy policies communicated to all workforce members?	No		🔴 Pending	

Question 1 – Enter Remediation:
Appoint a qualified workforce member to be responsible for the information security management program.

Question 2 – Enter Remediation:

Security Management Process (HIPAA Security Rule) - 164.308(a)(1)(i) Implement policies and procedures to prevent, detect, contain, and correct security violations.

Question 3 – Enter Remediation:
Maintaining security for protected health information is everyone's responsibility. Policies and procedures should be posted to an internal web site and workforce members should be required to read and understand their purpose.

BLUEPRINT HEALTHCARE IT

MeHI MASSACHUSETTS eHEALTH INSTITUTE

at the MassTech Collaborative

What’s on your mind?

Questions?

Contact Us

MeHI
MASSACHUSETTS
eHEALTH INSTITUTE

at the MassTech
Collaborative

🌐 mehi.masstech.org ☎ 1.855.MassEHR

✉ ehealth@masstech.org Follow us @MassEHealth