Privacy & Security Risk Analysis Webinar

BLUEPRINT HEALTHCARE IT

MeHI MASSACHUSETTS eHEALTH INSTITUTE at the MassTech Collaborative

Introduction: What We Do Matters

VISION

Massachusetts is the global eHealth leader. Our connected communities enjoy better health at lower cost and serve as models of innovation and economic development.

MISSION

To engage the healthcare community and catalyze the development, adoption and effective use of health IT

GOALS

Adoption

Support Health Reform

- Better Health
- Better Care
- Lower Costs

Consumer eHealth Engagement

Grow & Promote Innovation & eHealth Cluster

BLUEPRINT HEALTHCARE IT
MeHI MASSACHUSETTS eHEALTH INSTITUTE at the MassTech Collaborative

Massachusetts eHealth Institute (MeHI)

Support healthcare providers in achieving Meaningful Use of EHR technology

- Meaningful Use Gap Analysis
- Registration and Attestation support
- Secure document storage and audit preparation

Support providers with Physician Quality Reporting System (PQRS) reporting

- Qualified registry for submitting PQRS measures

Collaborate with external partners to offer

- Patient engagement resources
- Privacy and security tools – BluePrint SecurityConnect
- Other HealthIT resources

Engage in thought leadership

- Educational outreach, informational webinars and training courses
- Subject matter expertise on topics of interest to provider organizations

Disclaimer

- MeHI does not take any responsibility for the actions of physicians and their staff.
- MeHI acts as your trusted advisor for meaningful use and Health IT, and while MeHI will provide direction and connect you to appropriate privacy and security organizations and other services, physicians and their staff are solely responsible to take the steps necessary to protect the privacy and security of protected health information.

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 Principal Security Consultant for 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) certificate.

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.

Agenda

- Introductions
- Workshop Goals
- Introduction – BluePrint & Healthcare Landscape
- Regulatory/Compliance Landscape
- The Hard Truth!
- Security Rule
- Security Risk Analysis & Management
- Meaningful Use
- Myths about Security Rule and Meaningful Use
- MU Risk Analysis/Demo
- Q&A

Our Philosophy:

Our philosophy:

Make the process simple

Learning Objectives

After this session you will be able to:

- Understand the applicable state and federal laws/regulations
- Learn how to implement the HIPAA Security Rule and Meaningful Use (MU) in your organization
- Learn how to utilize BluePrint Healthcare IT's Security Connect for compliance with Security Rule/Meaningful Use

Healthcare Landscape

- Transition to electronic medical records
- Exchange of health information
- Meaningful Use
- ICD-10
- Affordable Care Organizations
- OCR (HIPAA) and CMS (Meaningful Use) Audits
- State and Federal Laws/Regulations (including penalties)

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.

201CMR17.00 17.04

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.

Knowledge Check

What types of information are considered personal information according to Massachusetts 201CMR17.00?

First Initial AND Last Name, PLUS:

- Social Security Number
- State-Issued ID (Driver's License, Photo ID)
- Account Number (even without PIN)

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

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

Global cost per incident in 2013

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

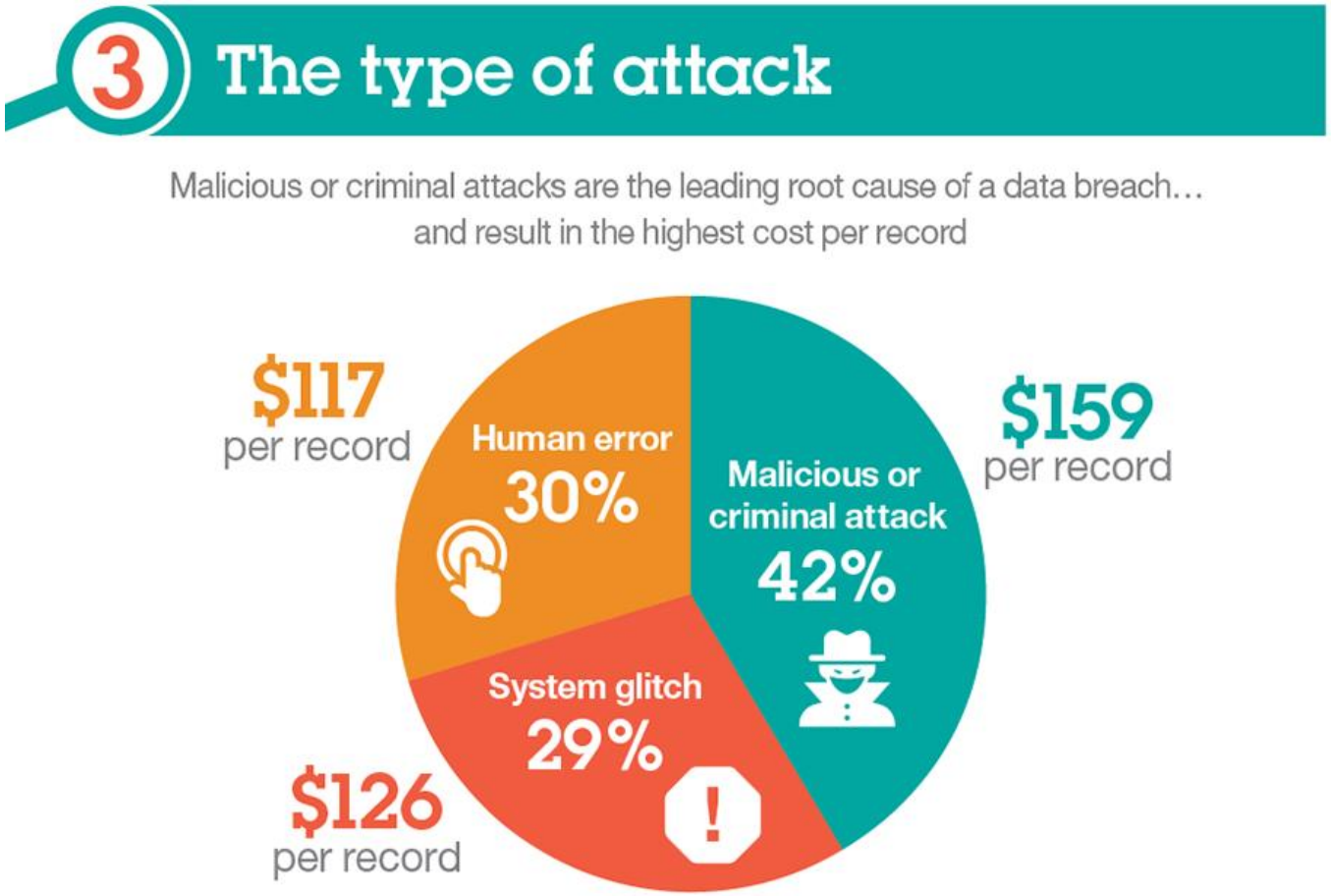
Highly regulated industries have the highest per-record cost of data breach

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

THIS is why we are here…

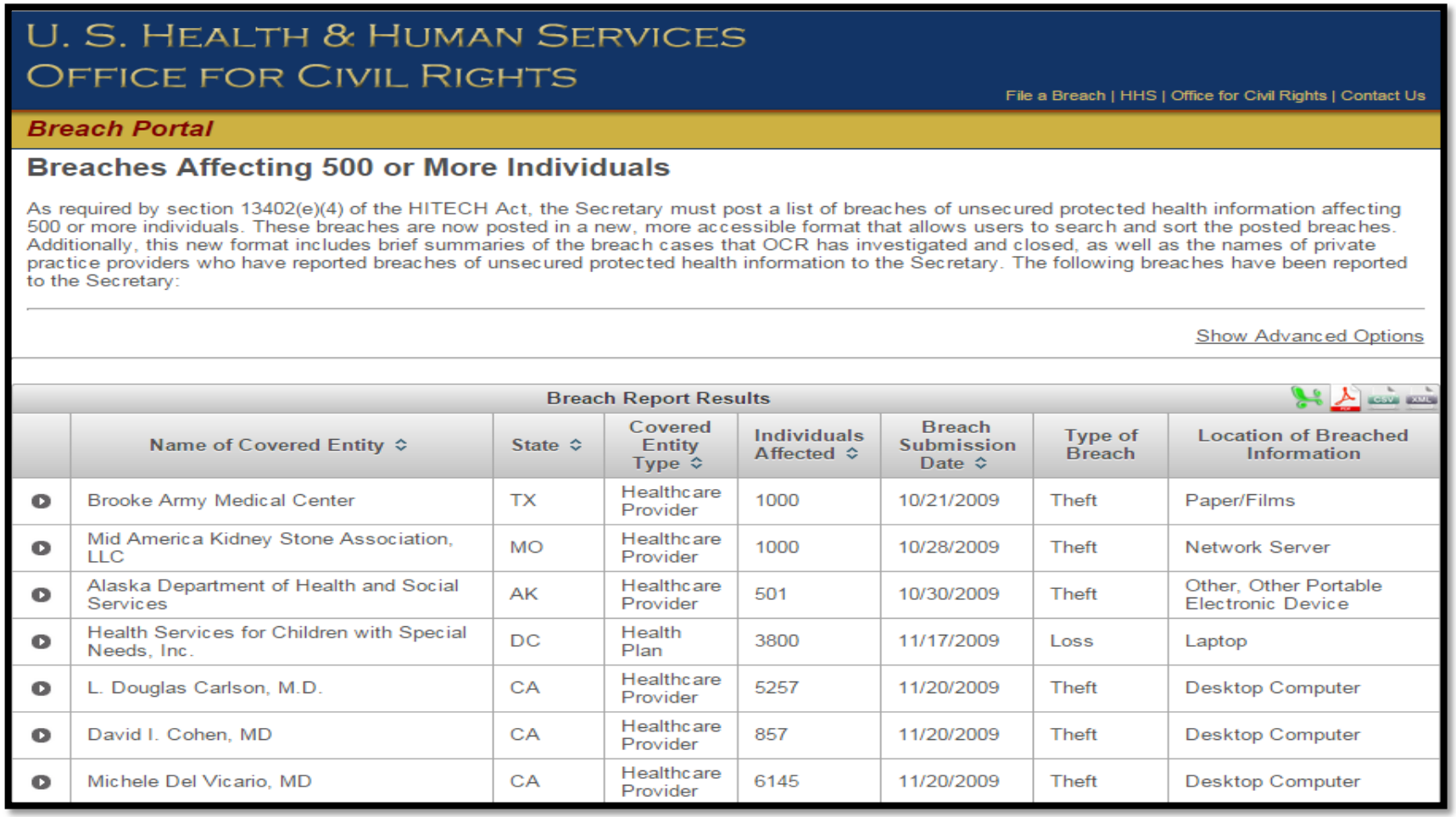
BLUEPRINT HEALTHCARE IT

MeHI MASSACHUSETTS eHEALTH INSTITUTE at the MassTech Collaborative



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

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 *1,142* reported breaches of 500 records or more since October 21, 2009

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

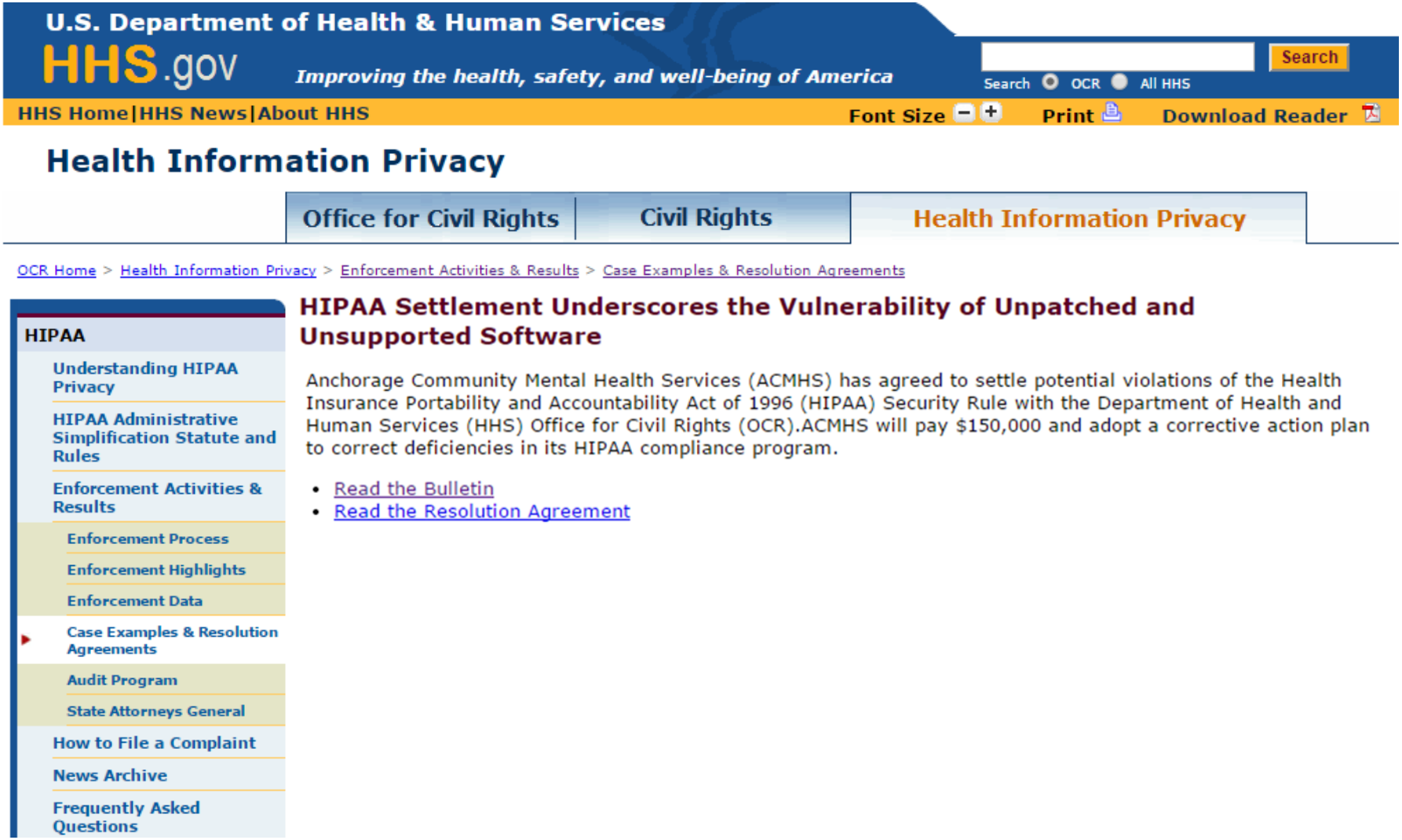
Columbia University (CU) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, including a $1,500,000 monetary settlement and corrective action plan to address deficiencies in its HIPAA compliance program.

- Read the Resolution Agreement
- HHS Press Release

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

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

BLUEPRINT HEALTHCARE IT

MeHI MASSACHUSETTS eHEALTH INSTITUTE at the MassTech Collaborative

HIPAA – Security Goal

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

HIPAA Security Risk Analysis – General Categories

ADMINISTRATIVE SAFEGUARDS

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangements

PHYSICAL SAFEGUARDS

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

TECHNICAL SAFEGUARDS

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

HIPAA Security Risk Analysis – General Categories

ORGANIZATIONAL REQUIREMENTS

- Business associate contracts or other arrangements
- Requirements for Group Health Plans

POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS

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

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

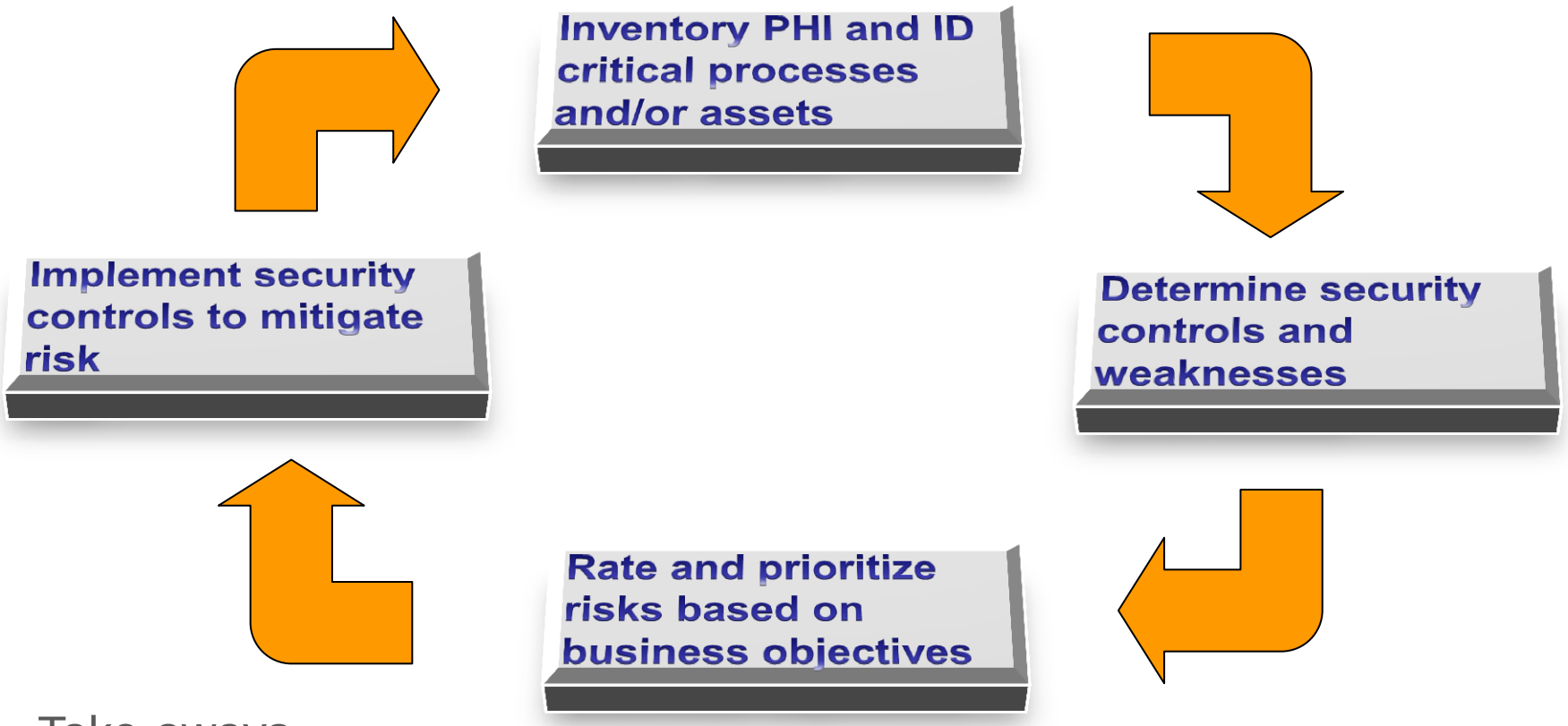
HIPAA Security Rule – Risk Analysis Guidance

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

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

HIPAA Security Rule – Risk Management Process



Take-aways

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

HIPAA Security Rule and Meaningful Use

In order to qualify under the Centers for Medicare and Medicaid Services (CMS) EHR incentive program, providers have to show that they are meaningfully using their EHRs by meeting thresholds for a number of objectives. The EHR Incentive Programs are phased in three stages* with increasing requirements.

Each phase includes the standards of conducting a Security Risk Analysis in accordance with the HIPAA Security Rule.

Meaningful Use – Stage 1

Stage 1 of the CMS EHR Incentive Program began in 2011. It sets the basic functionalities for EHRs. The requirements are focused on providers capturing patient data and sharing that data either with the patient or with other healthcare professionals.

Protect Electronic Health Information	
Objective	Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.
Measure	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.
Exclusion	No exclusion.

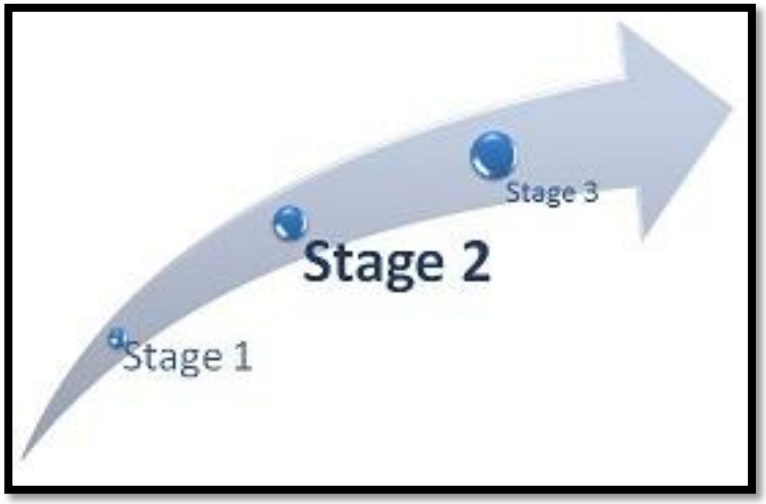
Meaningful Use – Stage 2

Stage 2 of the CMS EHR Incentive Program began in 2014. It uses advanced clinical processes. The requirements are focused on health information exchange between providers and promote patient engagement by giving patients secure online access to their health information.

Protect Electronic Health Information	
Objective	Protect electronic health information created or maintained by the certified EHR technology (CEHRT) through the implementation of appropriate technical capabilities.
Measure	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a) (1), including addressing the encryption/security of data stored in 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 provider's risk management process for EPs.
Exclusion	No exclusion.

Meaningful Use – Stage 3

Stage 3 of the CMS EHR Incentive Program is scheduled to begin in 2016 but the rule has not been finalized. Policy and Standards committees are developing recommendations to continue to expand meaningful use objectives to improve health care outcomes.



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

Knowledge Check

- **How often should I complete my Security Risk Analysis?**

  A full security risk analysis should be performed when you adopt an EHR. Thereafter, you should update the prior analysis for changes in risks every year, or whenever changes to your practice or electronic systems occur.

  To comply with HIPAA, you must continue to review, correct, modify, and update security protections. Under the Meaningful Use Programs, Eligible Professionals must conduct a security risk analysis prior to or during their EHR reporting period. A new review must be completed for each subsequent EHR reporting period. A security update is required if any security deficiencies were identified during the risk analysis.

Knowledge Check

- **My EHR vendor conducted a Security Risk Review. Is this sufficient to meet the Meaningful Use Core Measure?**

  Your EHR vendor may be able to provide assistance and training on the privacy and security aspects of the EHR. However, for Meaningful Use, it is your responsibility to complete a thorough security risk analysis, and to implement a plan to mitigate any security risks. Be sure to review not only your EHR hardware and software, but all electronic devices that store, capture, or modify electronic Protected Health Information (PHI). In addition, while your mitigation plan could include updates to your EHR software, it should also include changes in workflow processes or storage methods, and any other corrective action necessary to eliminate the security deficiencies identified in the risk analysis.

Knowledge Check

- **My organization has multiple locations. Do we need to conduct a separate Security Risk Analysis for each location?**

  A thorough Security Risk Analysis should take into account all of the electronic devices that store, capture, or modify electronic Protected Health Information (PHI). Because this may vary by location, a generic, organization-wide SRA may be insufficient. Your SRA should take into account all the variables that may impact the security of PHI for each specific location.

Risk Analysis – SecurityConnect Demo

MeHI's instance of SecurityConnect can be found at the following link:

https://securityconnect.bphitapps.com/mehi

MeHI Membership

Type of Service	# Providers	Pricing per Provider	Pricing per Practice
Remote MU Support	1 to 10	$699	NA
Remote MU Support	11 to 49	$629 (10% discount)	NA
Remote MU Support	50+	$559 (20% discount)	NA
Premium Services	NA	NA	$500

Type of Service	MeHI Members	Non-members
Privacy and Security Workshop (includes access to SecurityConnect Tool)	Free	$499/Provider
SecurityConnect Tool	Free	-

Join our Upcoming Workshop

The #1 reason providers are failing Meaningful Use audits is due to inadequate Security Risk Analysis

Get on track with your Security Risk Assessment and attest to Meaningful Use with MeHI's support & solutions:

- Assess your practice's privacy and security status
- Develop remediation plans to resolve gaps
- Communicate resolution steps to the providers involved
- Track progress in addressing outstanding issues
- Demonstrate compliance

Privacy & Security Workshop

Wednesday April 22, 2015

Cost: **Free** to MeHI Members
$499 for non-members

BLUEPRINT HEALTHCARE IT

MeHI MASSACHUSETTS eHEALTH INSTITUTE at the MassTech Collaborative

Q&A

Questions?

Contact Us

MeHI eHealth Services and Support
1-855-MASS-EHR
massehr@masstech.org
mehi.masstech.org

Thomas Bennett
Client Services Relationship Manager
(508) 870-0312 ext. 403
tbennett@masstech.org

BLUEPRINT HEALTHCARE IT

MeHI MASSACHUSETTS eHEALTH INSTITUTE at the MassTech Collaborative