HIPAA HITRUST and MARS-E

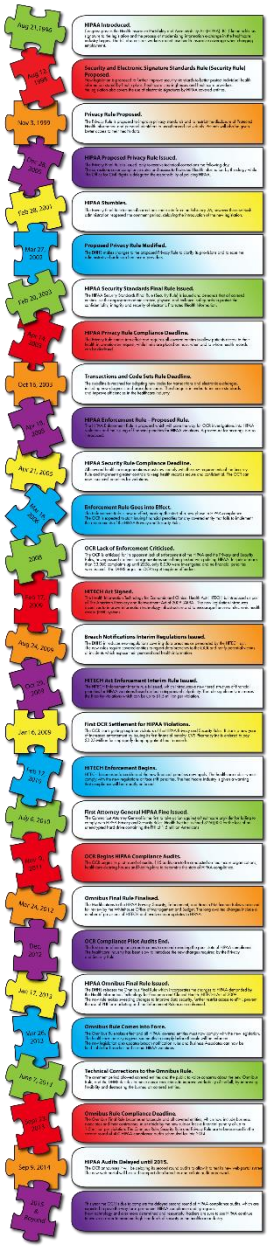
ControlCase Annual Conference 2016

Health Insurance Portability and Accountability Act - HIPAA

Administrative Simplification

- Electronic Transaction Standardization
- Privacy Rule
- Security Rule
- HITECH (ARRA) Provisions
- Omnibus Rule

Milestones of the Health Insurance Portability and Accountability Act.



Aug 21,1996

HIPAA Introduced.

Congress passes the Health Insurance Portability and Accountability Act (HIPAA). Bill Clinton adds his signature to the legislation and the process of modernizing information exchange in the healthcare industry begins. The bill also ensures workers do not lose health insurance coverage when changing employment.

Aug 12, 1998

Security and Electronic Signature Standards Rule (Security Rule) Proposed.

New legislation is proposed to further improve security standards to better protect individual health information stored by health plans, healthcare clearinghouses and healthcare providers. the legislation also covers the use of electronic signatures by HIPAA covered entities.

All breaches of ePHI affecting more than 500 individuals must be reported to OCR

Feb 17, 2009

HITECH Act Signed.

The Health Information Technology for Economic and Clinical Health Act (HITECH) is introduced as part of The American Recovery and Reinvestment Act of 2009 (ARRA). The new legislation introduces incentives to improve information technology infrastructure and to encourage the use of electronic health record (EHR) systems

Jan16, 2009

First OCR Settlement for HIPAA Violations.

The OCR starts getting tough on violators of the HIPAA Privacy and Security Rules. It starts a new year of increased enforcement by issuing its first financial penalty. CVS Pharmacy Inc is ordered to pay $2.25 Million for improperly dumping patient health records.

Nov 9, 2011

OCR Begins HIPAA Compliance Audits.

The OCR begins its pilot round of audits. 115 audits are to be conducted on healthcare organizations, healthcare clearing houses and health plans to determine the state of HIPAA compliance.

Sept 23, 2013

Omnibus Rule Compliance Deadline.

The Omnibus Final Rule becomes enforceable and all covered entities, which now include business associates and their contractors, must abide by the new rule or face a financial penalty of up to 1.5 million per violation. The Omnibus Rule, Security Rule and Privacy Rule are to be assessed in the second round of 400 HIPAA compliance audits scheduled for late 2014.

Business Associates Covered

HIPAA Risks

- Complaints filed by anyone online, fax or email
- Random OCR Audits
- Breaches and related fines

HIPAA Resolution Actions

- $2.14 million HIPAA settlement underscores importance of managing security risk - **October 18, 2016**
- HIPAA settlement illustrates the importance of reviewing and updating, as necessary, business associate agreements $400K fine – **September 23, 2016**
- Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million **- August 4, 2016**
- Multiple alleged HIPAA violations result in $2.75 million settlement with the University of Mississippi Medical Center (UMMC) - July 21, 2016
- Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University - July 18, 2016
- Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to $650,000 HIPAA Settlement – June 29, 2016
- Unauthorized Filming for "NY Med" Results in $2.2 Million Settlement with New York Presbyterian Hospital - April 21, 2016
- $750,000 settlement highlights the need for HIPAA business associate agreements
- Improper disclosure of research participants' protected health information results in $3.9 million HIPAA settlement - March 17, 2016
- $1.55 million settlement underscores the importance of executing HIPAA business associate agreements - March 16, 2016
- Physical therapy provider settles violations that it impermissibly disclosed patient information $25K- February 16, 2016
- Administrative Law Judge rules in favor of OCR enforcement, requiring Lincare, Inc. to pay $239,800 - February 3, 2016
- $750,000 HIPAA Settlement Underscores the Need for Organization Wide Risk Analysis - December 14, 2015
- Triple-S Management Corporation Settles HHS Charges by Agreeing to $3.5 Million HIPAA Settlement - November 30, 2015

SOURCE - http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

What do people do – whatever they can

- Misconfigured web application – Cost $2.7 million
- Lost laptop in a train – Cost $1 million
- Forgot to update the BAA (a few lines were missing) – Cost $400K
- Patient testimonials on a website – Cost $25K
- Dumped 800 medical records in the trash – Cost $800K
- Unpatched and Unsupported software - Cost $150K
- Internet based publicly available calendar – Cost $100K
- Photocopier lease ends – Cost $1.2 million
- Stolen laptop – Cost $1.72 million

HIPAA Items


Risk Analysis
Risk Management Plan
Availability and Disaster Recovery
Integrity
Training
Access Control
Logging Monitoring
Incident Response
Contracts
Physical Security
Encryption

Disclosed Data Breaches of 500 or more individuals

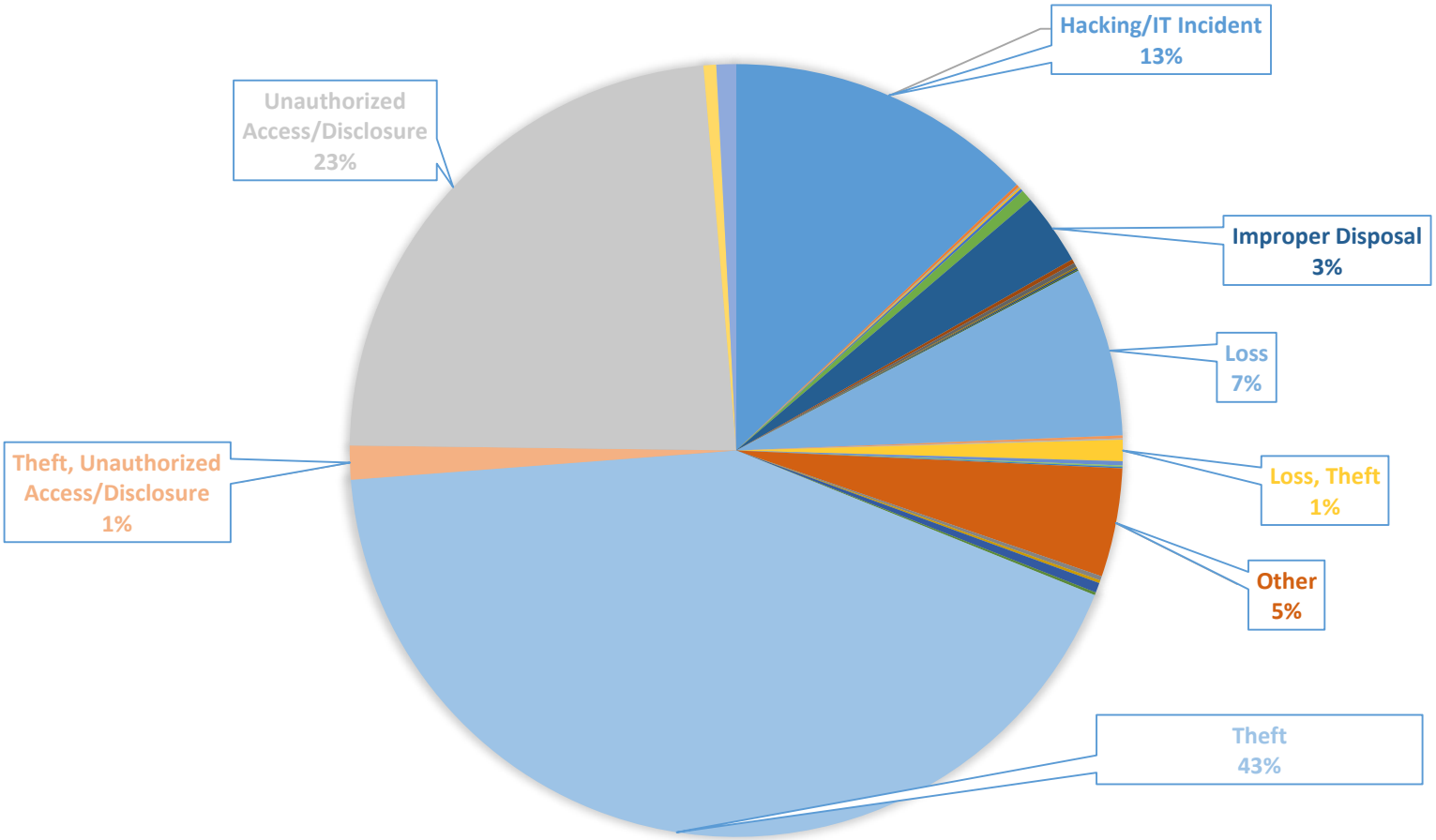
1694 Reported Breaches from 10/21/2009 to 10/10/2016

169 MILLION individuals affected

Theft is the biggest cause of breaches

Number of incidents have been steady - between 200 to 300 a year - Every Year

Types of Breaches



Some more numbers

Year	Sum of Individuals Affected
<10/21/2009	
2009	134,773
2010	5,534,276
2011	13,150,298
2012	2,808,042
2013	6,950,118
2014	12,737,973
2015	113,267,174
2016	14,255,460
Grand Total	168,838,114

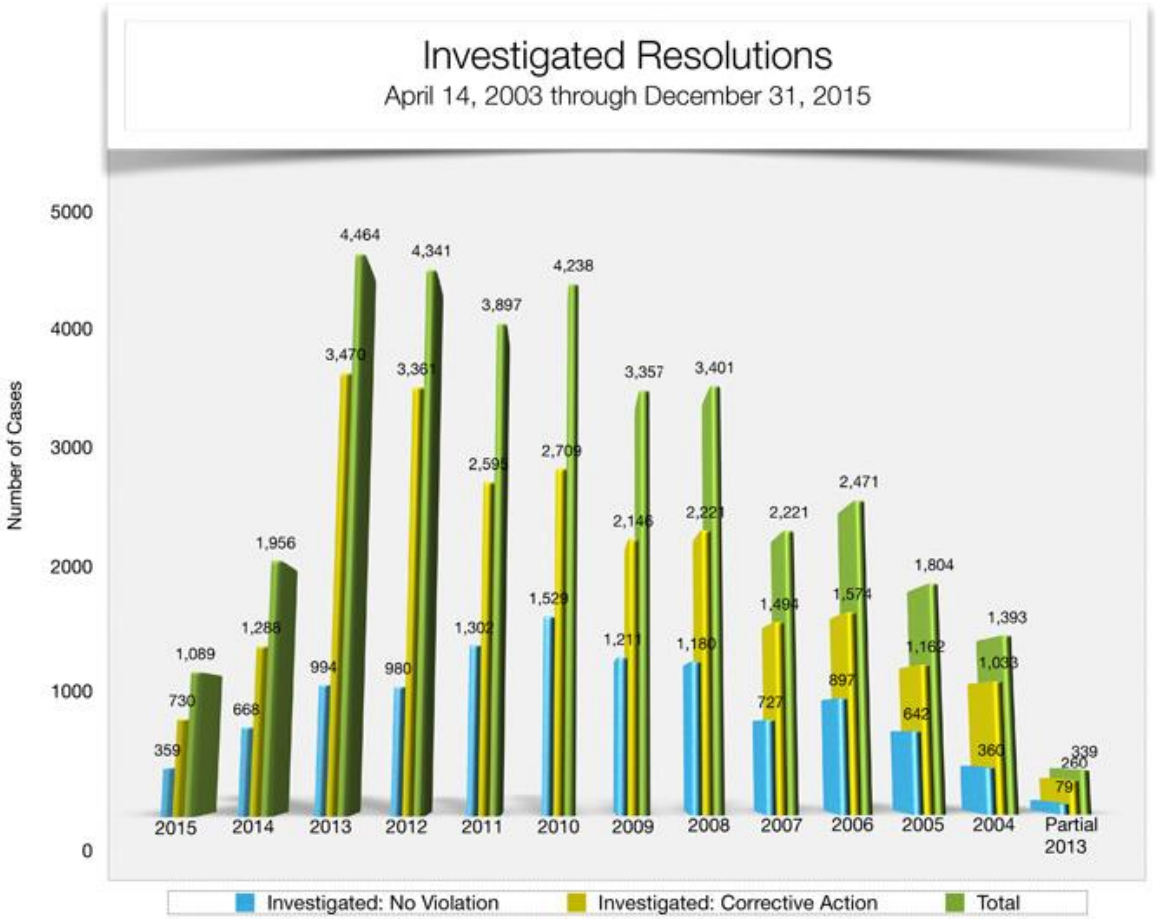
Covered Entity Type	Individuals
Business Associate	28,584,393
Health Plan	109,047,676
Healthcare Clearing House	17,754
Healthcare Provider	30,945,362

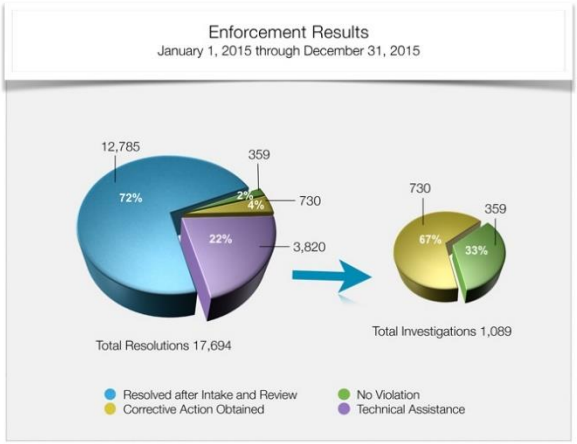
Year	Number of Incidents
<10/21/2009	
2009	18
2010	198
2011	195
2012	201
2013	267
2014	290
2015	267
2016	235
Grand Total	1,671

Top 10 Entities

Name of Covered Entity	State	Covered Entity Type	Individuals Affected
Anthem, Inc. Affiliated Covered Entity	IN	Health Plan	78,800,000
Premera Blue Cross	WA	Health Plan	11,000,000
Excellus Health Plan, Inc.	NY	Health Plan	10,000,000
Science Applications International Corporation (SA	VA	Business Associate	4,900,000
Community Health Systems Professional Services Corporation	TN	Business Associate	4,500,000
University of California, Los Angeles Health	CA	Healthcare Provider	4,500,000
Advocate Health and Hospitals Corporation, d/b/a Advocate M	IL	Healthcare Provider	4,029,530
Medical Informatics Engineering	IN	Business Associate	3,900,000
Banner Health	AZ	Healthcare Provider	3,620,000
Newkirk Products, Inc.	NY	Business Associate	3,466,120

Fines and Corrective Actions





HITRUST CERTIFICATION

Health Information Trust Alliance

HITRUST

- Provides the CSF an Information Security Framework used to certify for HIPAA
- Helps quantify the regulation into a set of measurable goals

What's missing in HIPAA

164.308a1i - Security management process
Implement policies and procedures to prevent, detect, contain, and correct security violations.

164.308a5B - Protection from malicious software:
Procedures for guarding against, detecting, and reporting malicious software

164.308a1iiA - Risk Analysis:
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.

164.308a7iiB – Disaster Recovery Plan:
Establish (and implement as needed) procedures to restore any loss of data.

164.308a5B Procedures for guarding against, detecting, and reporting malicious software

Type:	Organizational
Level:	1
Related HITRUST CSF Control:	09.j Controls Against Malicious Code
Scope:	In scope
HITRUST CSF Requirement Statement:	Anti-virus and anti-spyware are installed, operating and updated on all devices to conduct periodic scans of the system to identify and remove unauthorized software.

Illustrative Procedures	
Policy:	Obtain and examine the malware protection policies to determine if requirements are defined for the installation, operation and update of anti-virus and anti-spyware software on all devices, and the performance of periodic scans on electronic or optical media, files received over networks, electronic mail attachments, downloads, and web traffic to identify and remove malicious software.
Process:	Obtain and examine the malware protection procedure documentation to determine if a process is defined for the installation, operation and update of anti-virus and anti-spyware software on all devices, and the performance of periodic scans to identify and remove malicious software.
Implemented:	Interview the individual(s) responsib installation, operation and update o to identify and remove malicious so (desktops, laptops, servers, etc.), de
Measured:	Interview key personnel to determir spyware software is installed, opera malicious software.
Managed:	Obtain and examine supporting doc identified were investigated and cor

Type:	Organizational
Level:	1
Related HITRUST CSF Control:	09.j Controls Against Malicious Code
Scope:	In scope
HITRUST CSF Requirement Statement:	Audit logs of the scans are maintained.

Illustrative Procedures	
Policy:	Obtain and examine the malware protection policies to determine if requirements are defined for maintaining audit logs of the malicious software scans.
Process:	Obtain and examine the malware protection procedure documentation to determine if a process is defined for maintaining audit logs of the malicious software scans.
Implemented:	Interview the individual(s) responsible for malware protection to determine if a process has been implemented for maintaining audit logs of the malicious software scans in accordance with the documented procedures. For a sample of endpoint devices (desktops, laptops, servers, etc.), determine if audit logs of all scans performed are maintained.
Measured:	Interview key personnel to determine if reviews, tests or audits are completed by the organization to verify audit logs are maintained of the malicious software scans.
Managed:	Obtain and examine supporting documentation maintained as evidence of these reviews, tests or audits to determine if issues identified were investigated and corrected.

MARS-E

Minimum Acceptable Risk Standards for Exchanges

MARS-E - Minimum Acceptable Risk Standards for Exchanges

- Addresses the mandates of the Patient Protection and Affordable Care Act of 2010
- The purpose of MARS-E is to **provide security information aimed to protect and ensure the confidentiality, integrity and availability** of Personally Identifiable Information (PII), Protected Health Information (PHI) or Federal Tax Information (FTI) of enrollees of Administering Entities.
- MARS-E 2.0 is comprised of security updates that respond to the National Institute of Standards and Technology (NIST) updates and the evolving technology and threat space such as mobile and cloud computing, insider threat, applications security, advanced persistent threat, supply chain risks, trustworthiness, assurance and resilience of systems

Who is covered

Applies to all **Affordable Care Act Administering Entities** (AEs) to include

- Exchanges or Marketplaces, whether Federal or State
- Medicaid Agencies
- Children's Health Insurance Program (CHIP) agencies
- State agencies administering the Basic Health Program (BHP)
- **All contractors and subcontractors**

MARS-E Suite

MARS-E 2.0 is a suite of four documents:

- **Harmonized Security and Privacy Framework**: This is a high-level **introduction of Affordable Care Act Security and Privacy policy** and standards as a framework for compliance governance.
- **Minimum Acceptable Risk Standards for Exchanges**: This volume introduces the **concept of a Catalog of Controls; one catalog for security and another for privacy**. This volume also has two appendices: 1) Security Controls Selection Table, showing MARS-E V1.0, NIST 800-53 Rev4 Moderate Baseline, ARS 2.0, and MARS-E V2.0 control set; and 2) Mapping of 45 CFR §155.260 to MARS-E Security and Privacy Controls.
- **Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges:** This volume contains the **security and privacy control tables**. It also contains the IRS Requirements for Safeguarding FTI in Appendix A.
- **ACA Administering Entity System Security Plan**: This is a consolidated volume containing **System Security Plan (SSP) Instructions** and fill-in the blanks Page 3-CMCS Informational Bulletin template for SSP Content.

Thank You !