

# HIPAA... The Rules Have Changed

Cathie Brown, CGEIT, PMP, CISM, CISSP  
September 28, 2010



eHealthSecurity

# Agenda

- Speaker Introduction
- HIPAA... Quick Review
- HIPAA... Fast Forward
- HIPAA... The Rules Have Changed
- HIPAA... Goes HITECH
- Meaningful Use... and Stimulus
- Q&A



# Speaker Introduction

- 20+ Years in Information Technology
- 18 Years in Healthcare IT
- Former Deputy Chief Information Security Officer of the Commonwealth of Virginia
- President, IT Governance Solutions, LLC
- Partner, eHealthSecurity
- CGEIT (Certified in Governance of Enterprise IT)
- PMP (Project Management Professional)
- CISM (Certified Information Security Manager)
- CISSP (Certified Information Security Systems Professional)

# HIPAA ... Quick Review

## Health Insurance Portability and Accountability act of 1996

Title I Health  
Care Access  
Portability and  
Renewability

Title II Administrative Simplification; Fraud and Abuse Prevention

Title III Tax  
Related Health  
Provisions

Title IV  
Application  
and  
Enforcement  
of Group  
Health Plan  
Requirements

Title V  
Revenue  
Offsets

Transactions

Code Sets

Unique Health  
Identifiers

Privacy

Security



eHealthSecurity

# HIPAA Privacy Review

ADMINISTRATIVE REQUIREMENTS (164.530)	STATUS
Determine Covered Entity status	✓
Designate a Privacy Official	✓
Identify Business Associates and enter Business Associate Agreements	✓
Compare current PHI use and disclosure practices with Privacy Rule requirements, and identify where practices need to change	✓
Identify "TPO" uses and disclosures of PHI, all other uses and disclosures (e.g., public policy), and develop Minimum Necessary policies and protocols	✓
Develop and provide a Notice and, if necessary, an Acknowledgment form	✓
Develop a system to track and account for disclosures	✓
Design and Implement Policies and Procedures	✓
Train workforce	✓
Develop and apply a system of sanctions for employees who violate the entity's policies or the requirements of the Privacy Rule	✓



# HIPAA Security Review

ADMINISTRATIVE SAFEGUARDS	SECTIONS	SPECIFICATIONS
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Clearance/Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Function (R) Access Authorization (A) Access Establishment/Modification (A)
Security Awareness and Training	164.308(a)(5)	Security reminders (A) Protection from Malicious Software (A) Log-In Monitoring (A) Password Management (A)
Security incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)



# HIPAA Security Review

PHYSICAL SAFEGUARDS	SECTIONS	SPECIFICATIONS
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)



# HIPAA Security Review

TECHNICAL SAFEGUARDS	SECTION	SPECIFICATION
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate EPHI (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)



# HIPAA... Fast Forward

- American Recovery and Reinvestment Act of 2009
  - ARRA passed on February 17, 2009
  - Title XIII - Health Information Technology for Economic and Clinical Health Act (HITECH)
  - Data Breach Notification
  - Business Associates subject to HIPAA
  - Increased Penalties and Enforcement
  - “Meaningful Use” and Stimulus Funding



# HIPAA... The Rules Have Changed

- NPRM: Proposed Rule published July 14, 2010  
**“HITECH: Modifications to the HIPAA Privacy, Security and Enforcement Rules”**
- Public Comment Period ended 9/13/2010
- Compliance required 180 days after the final rule is published in the Federal Register

# Rule Changes

- Data Breach Notification
  - Covered Entities are required to provide notification to individuals if PHI is breached (Section 13402)
- Business Associates
  - Business Associate's must Comply with HIPAA and Clarification of Who is a Business Associate (Section 13401, 13404)
- Right to Restrict Disclosures
  - Individuals have the right to request a restriction on certain uses and disclosures of their PHI (Section 13405 (a))

# Rule Changes

- **Electronic Access**
  - Individuals have the right to access and obtain a copy of their health records (Section 13405 (e))
- **Marketing and Fundraising**
  - When Authorization is Required for Marketing Communications (Section 13406 (a))
  - Opt-Out for Fundraising Communications (Section 13406 (b))
- **Accounting for Disclosures**
  - Covered Entities must provide to an individual, upon request, an accounting of disclosures (Section 13405 (c))

# Enforcement Rule Changes

- Application of Criminal Penalties (Section 13409)
  - Covered Entities **and individuals, including employees** of a Covered Entity may be prosecuted for HIPAA violations
- When Civil Penalties Can (or Must) be Pursued (Section 13410)
  - HHS Secretary AND state Attorney General are **required** to formally investigate and impose penalty if violation is found
- Increase in Civil Monetary Penalties (Section 13410 (d))
  - Tiered Structure up to \$50,000/per violation; max of \$1.5 million/year (rather than \$100/\$25,000)
- Secretary's Audit Authority (Section 13411)
  - Secretary to perform **mandatory periodic audits** to ensure compliance to Privacy and Security Rules

# HIPAA goes HITECH

- Administration Changes
  - Office of the National Coordinator for Health IT (ONCHIT) established
  - HIT Policy Committee
    - Required to make recommendations with respect to technologies that protect privacy and promote security in an electronic health record, including those that allow for the segregation of sensitive health information and the use of limited data set
    - Prioritize the development of standard to facilitate the new accounting for disclosures
  - HIT Standards Committee
  - Chief Privacy Officer within ONC



# Meaningful Use...and Stimulus

- Allows approximately \$31.2 billion for healthcare infrastructure and adoption of EHR
  - Non-hospital based physicians
    - Up to \$44,000 (Medicare)
    - Up to \$64,000 (Medicaid)
  - Hospitals with Medicare and Medicaid
    - Up to \$11 Million

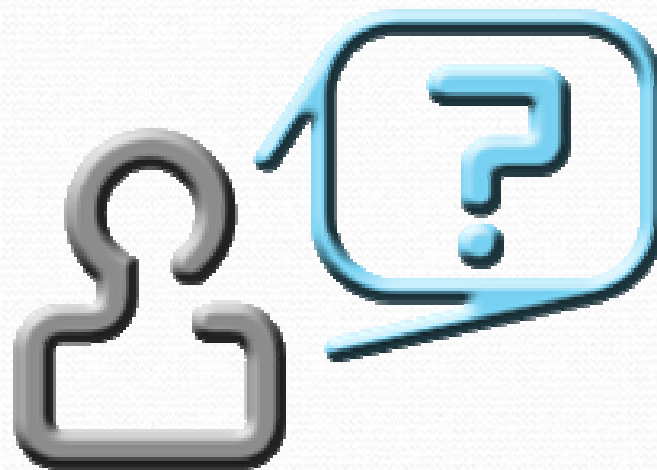
\* Paid out over a 4 to 5 year period beginning in 2011



# Recap

- Compliance to the existing HIPAA Privacy and Security Rules still applies and is **Mandatory**
- ARRA passed in 2009 included HITECH (Title XIII)
- Included revised/additional requirements for Healthcare Privacy & Security & **Enforcement**
- NPRM for Modifications to the HIPAA Privacy, Security and Enforcement Rules is being finalized
- HIPAA Compliance is key for meeting 'Meaningful Use'

# Questions



**Cathie Brown**  
**(434) 665-0345**

**[ctbrown@eHealthSecurity.info](mailto:ctbrown@eHealthSecurity.info)**  
**[www.eHealthSecurity.info](http://www.eHealthSecurity.info)**



**eHealthSecurity**

# HIPAA Security

Bryan Miller, CISSP  
September 28, 2010



**eHealthSecurity**

# Agenda

- Speaker Introduction
- Threats to PHI
- Real World Examples
- What Have We Learned
- Q&A



# Speaker Introduction

- B.S. – Information Systems – VCU
- M.S. – Computer Science – VCU
- President, Syrinx Technologies & Partner at eHealthSecurity
- Member of HIMSS, ISSA & InfraGard
- Former Adjunct Faculty in Information Systems & Computer Science at VCU
- Former Lecturer at VCU Fast Track Executive Master of Science (FTEMS) Program



# Threats to PHI

- Web applications continue to grow in complexity.
- Applications are written with security as an afterthought.
- New vulnerabilities are discovered every day.
- Exploits have become easy to obtain and use.



# Threats to PHI

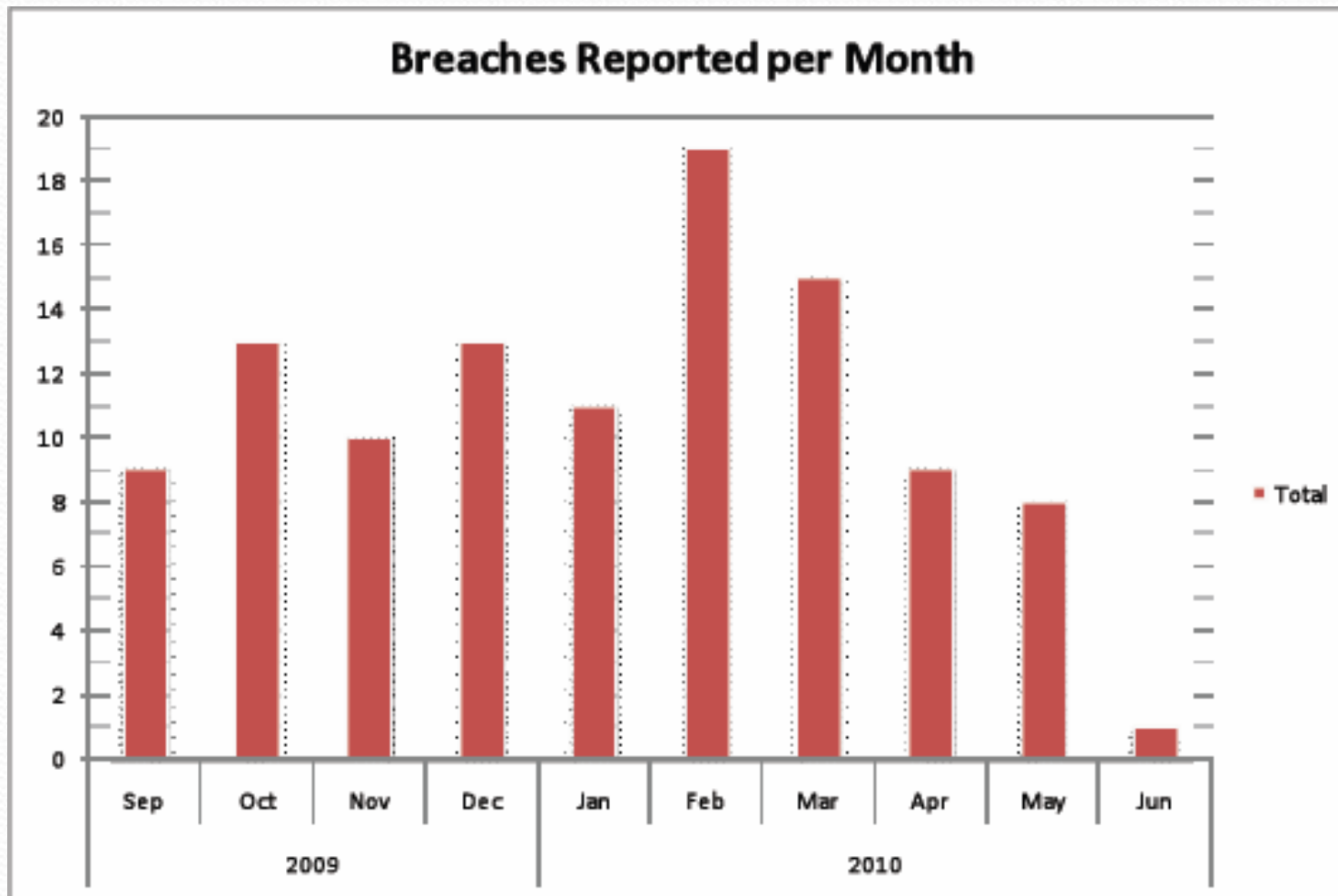
- The Health Information Trust Alliance published an analysis in August:
  - **108 breaches** were reported in **10 months** (Sept. 23, 2009, to mid-July 2010)
  - **4,089,670 individuals** and **health records** affected
  - Health plans and physician practices were the biggest targets



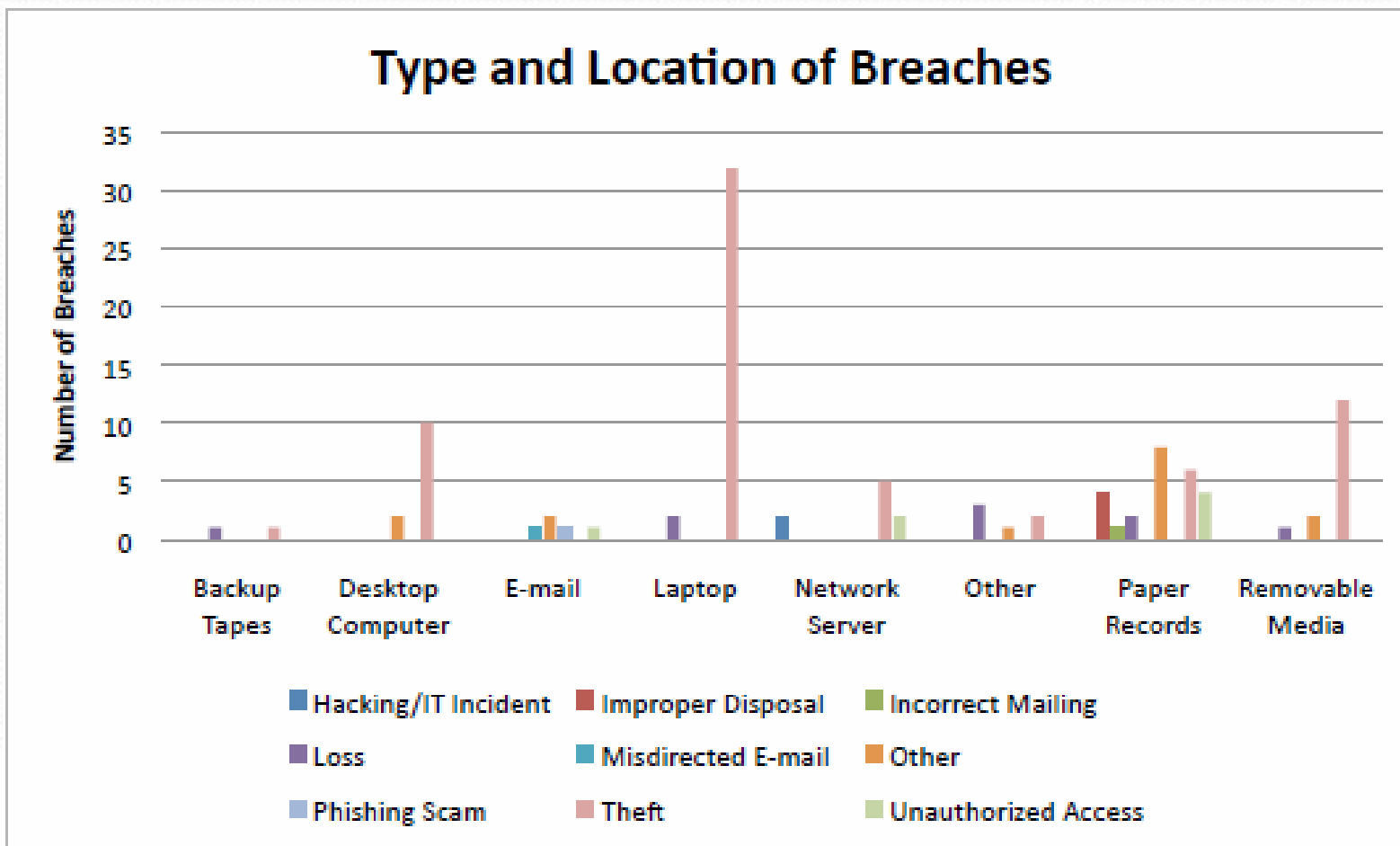
eHealthSecurity

Source: [www.hitrustcentral.net/blogs/ht/archive/2010/08/02/update-an-analysis-of-hhs-breach-data.aspx](http://www.hitrustcentral.net/blogs/ht/archive/2010/08/02/update-an-analysis-of-hhs-breach-data.aspx)

# Threats to PHI



# Threats to PHI



# Real World Examples

- May 2010 – KPMG LLP loses unencrypted flash drive from Saint Barnabas Health Care System (3,630 patients)
- May 2010 – SunBridge Healthcare loses laptop with resident data from 10 states
- July 2010 – Cooper University Hospital lost a flash drive containing employee information
- July 2010 – Virginia psychiatrist had a laptop stolen containing patient data (2,739 patients)



# Real World Examples

- July 2010 – Pediatric and Adult Allergy loses a backup tape containing client data
- July 2010 – Theft of a desktop belonging to E. Brooks Wilkins Family Medicine (13,000 patients)
- August 2010 – SunBridge Healthcare loses unencrypted Blackberry (1,000 patients)
- August 2010 – Yale Medical School has a laptop stolen (1,000 patients)



# What Have We Learned

- Policy & Procedures
  - Lack of proper physical security
  - Sensitive data stored without encryption
  - Sensitive data transmitted/stored in email



# What Have We Learned

- Patch Management
  - Verify that patches are actually applied
  - Make sure to patch desktops and servers
  - Make sure to patch operating systems and applications
  - Don't forget appliances and other network infrastructure devices



# What Have We Learned

- Password Management
  - Blank passwords
  - Default database passwords
  - Common passwords across different platforms and/or architectures



# What Have We Learned - Recap

- The 3 P's
  - Policies & Procedures
  - Patch Management
  - Password Management
- The majority of the remediation efforts are not costly in resources (human, technology, financial)
- The biggest changes have to occur with users, systems administrators and developers



# Questions

Bryan Miller

804-539-9154

[bryan@ehealthsecurity.info](mailto:bryan@ehealthsecurity.info)

[www.ehealthsecurity.info](http://www.ehealthsecurity.info)



**eHealthSecurity**