A Glimpse Into Privacy and Security: Where Have We Been and Where Are We Going

Danika E. Brinda, MA, RHIA, CHPS
Assistant Professor/HIT REACH Consultant
The College of St. Scholastica

Thursday, March 21, 2013

HIPAA in the News

Feds Go to Court to Collect First-Ever Fine for HIPAA Violations

Featured in Health Business Daily, Aug. 18, 2011, and in Government News of the Week,

In February, the Office for Civil Rights imposed a $4.3 million fine on a Maryland medical group tha had refused to honor 41 patients' requests for their medical records…"

Medical Billing Firm Says Personal Information Leaked to Theft Ring

www.ihealthbeat.org, December 3, 2012

"Advanced Data Processing said that an employee improperly accessed individual account data in the company's ambulance billing system and leaked the information to a theft ring. The worker has admitted to the crime and has been fired…"

Text Message Use Among Providers Raise HIPAA Concerns

Written by Joyce McLaughlin, JD, Senior Counsel, Davis & Wilkerson ,August 11, 2011,http://www.beckershospitalreview.com

"As the possibilities for electronic communication continue to expand with great speed, use of the technology by hospital employees and physicians without adequate security can expose your facility to HIPAA violations. The increasing use of cell phones and texting …"

9 Patients' Identities Stolen in Emory Healthcare Data Breach

Written by Sabrina Rodak| October 25, 2011 | http://www.beckershospitalreview.com

"Nine patients of Emory Healthcare's orthopedic clinic in Tucker, Ga., have had fraudulent tax returns filed in their name, according to a Channel 2 report. The nine patients were among 32 Emory orthopedic clinic patients whose hospital bills were stolen in April…"

2012 Security Breaches

Some 57,000 patients seen at the Palo Alto, Calif.-based Lucile Packard Children's Hospital have been notified of a potential HIPAA-breach after an unencrypted company laptop containing patient medical information was stolen from a physician's car Jan. 9.

In the Lake County case, an unauthorized remote user posted a message on the practice's server stating that its contents had been encrypted and could only be accessed with a password. The hackers would give the surgeons the password ... in exchange for a ransom. (The docs did not pay–instead they turned off the server and called the police)

Students at Stanford University setup secret identities so they can post information about patients on Facebook and other social media sites

...posted a picture of a patient's medical record on his Facebook account, saying it was "funny" that the patient "came in to cure her VD and get birth control." When commenters protested, he responded, "People, it's just Facebook. ... It's ns of names. If some people can't appreciate on't like it, too bad because it's my wall, and

The Veteran's Administration reported 173 incidents of security breaches of medical devices from 2009-11 that disrupted glucose monitors, canceled patient appointments and shut down sleep labs.

In this case, old operating systems are often to blame–it's a matter of keeping virus software up-to-date and hospitals are working with vendors to fix that threat. But it's not always possible to patch old systems, which means a big bill to fix this problem will inevitably be coming due.

Source: http://www.hipaasecurenow.com/index.php/blog/

Top 2012 Data Breaches

COVERED ENTITY	INDIVIDUALS AFFECTED	TYPE OF BREACH	LOCATION OF BREACHED INFORMATION
Utah Department of Health	780,000	Hacking/IT Incident	Network Server
Emory Healthcare	315,000	Unknown	Backup Disks
South Carolina Department of Health and Human Services	228,435	Unauthorized Access/Disclosure	Email
Alere Home Monitoring, Inc.	116,506	Theft	Laptop
Memorial Healthcare System	102,153	Theft	Electronic Medical Record

Source: http://www.dolbey.com/uncategorized/redspin-2012-health-data-breach-report-breakdown/

Utah Re… Calif. Hospital Reports Data Breach Affecting 6,000 Me… About 57K Patients

The Utah D… beneficiarie… the *Salt La…*

The recent… stole perso… beneficiarie…

Details of …

On Jan. 10… contractor … program -- … drive (Stew…

The employ… City, Denve…

Patient dat…

- Names;
- Ages;
- Medica…
- Prescrip…

The thumb… information…

Lucile Packard Children's Hospital in Palo Alto, Calif., and the Stanford University School of Medicine are notifying about 57,000 patients about a data breach that occurred Jan. 9, *Healthcare IT News* reports.

The recent incident follows three other data breach incidents at Lucile Packard or Stanford University Medical Center since 2010 (McCann, *Healthcare IT News*, 1/23).

Details of the Incident

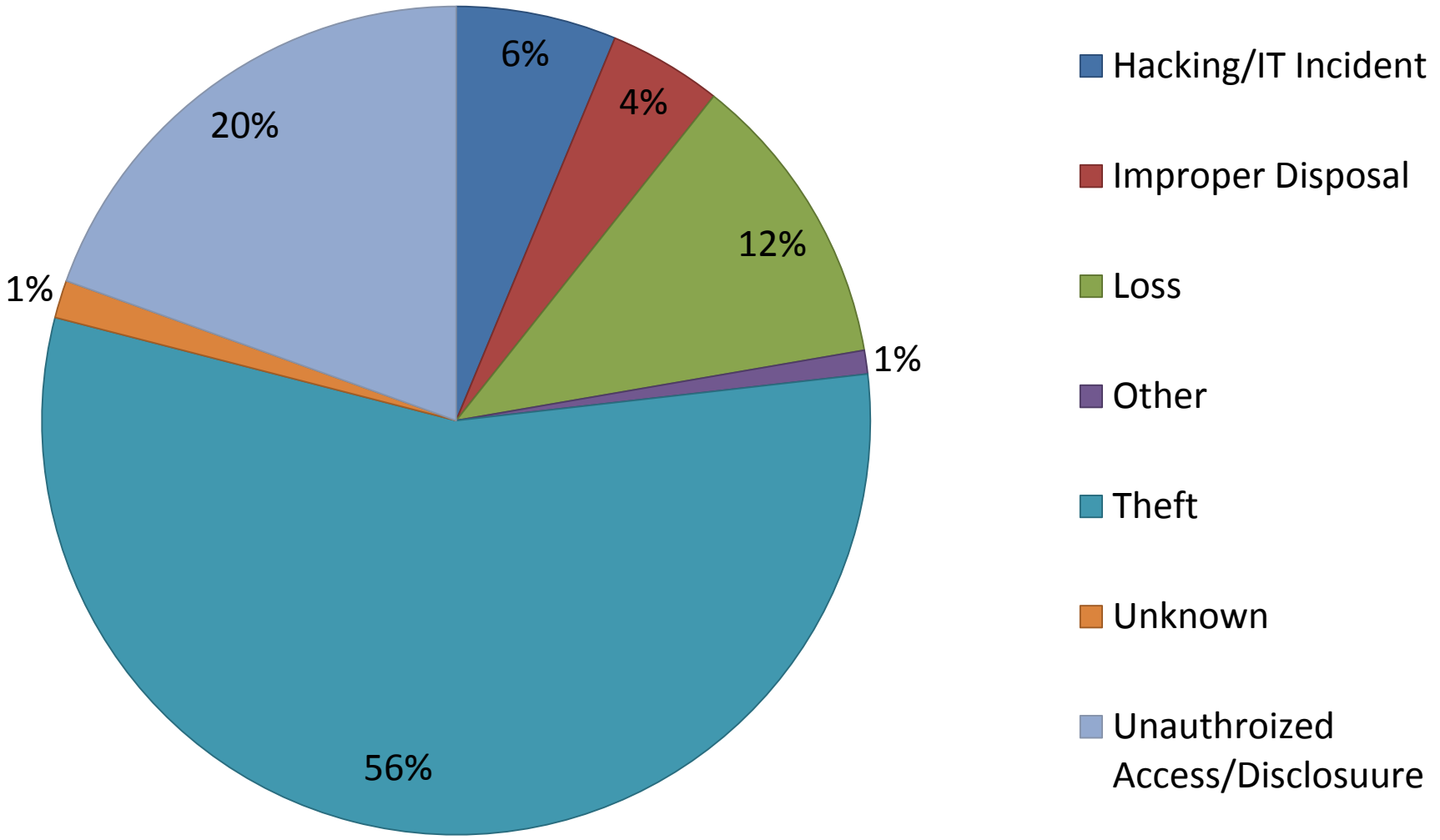
On Jan. 9, a password-protected laptop computer with limited medical data about pediatric patients was stolen from a physician's car.

Information on the laptop primarily was from 2009 and pertained to past care and research (Roney, *Becker's Hospital Review*, 1/23).

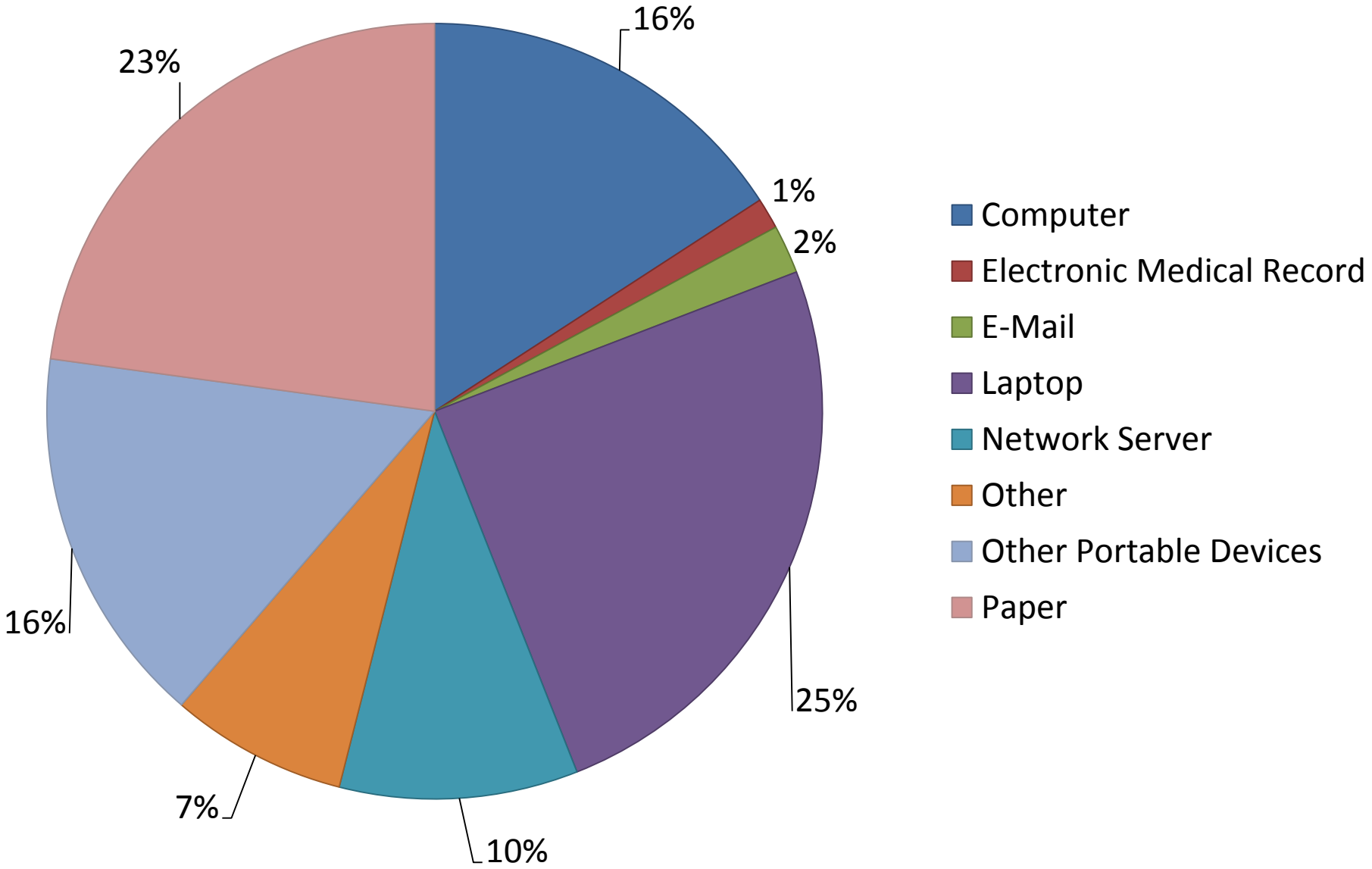
On Jan. 10, the incident was reported to Lucile Packard. Patient data stored on the laptop included:

- Names;
- Dates of birth;
- Health record numbers; and
- Certain clinical data (*Healthcare IT News*, 1/23).

Breach by Type
September 2009 - December 2012

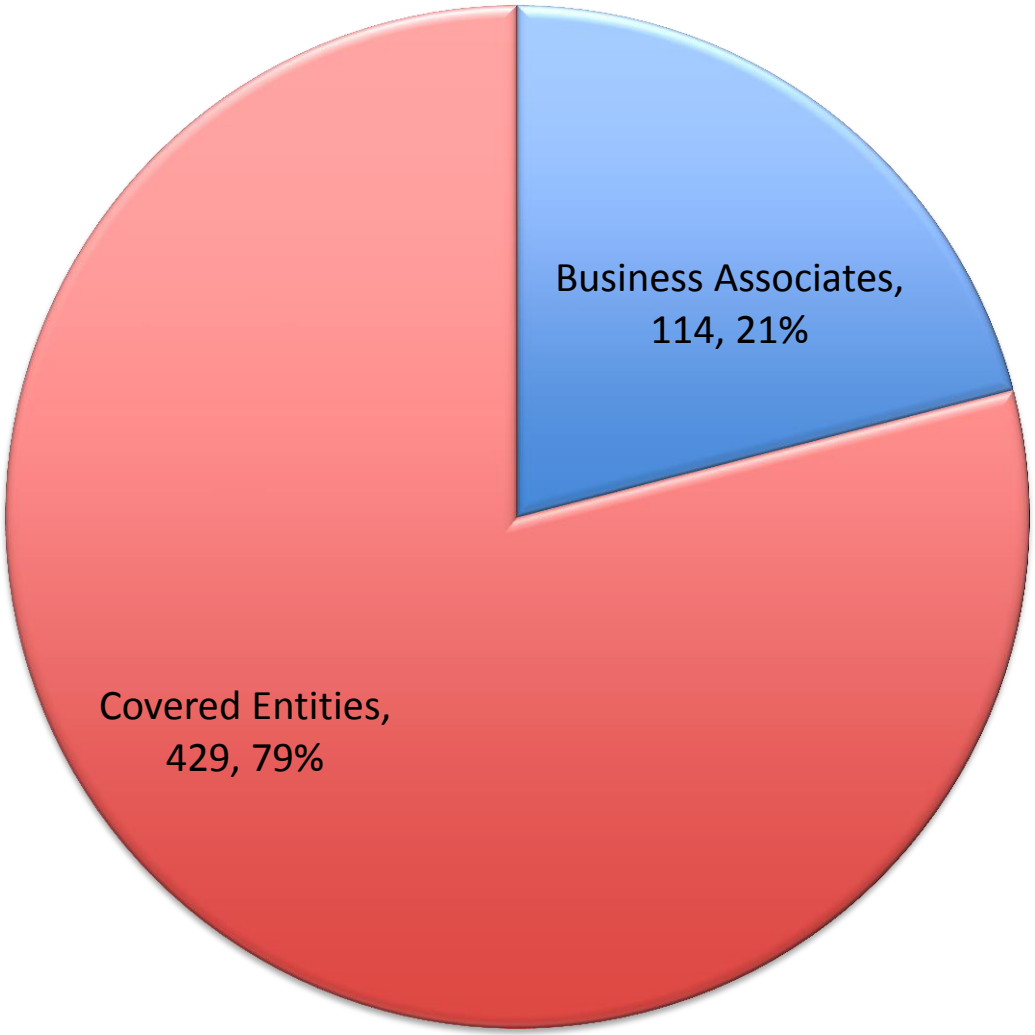


Location of Breach
September 2009 - December 2012

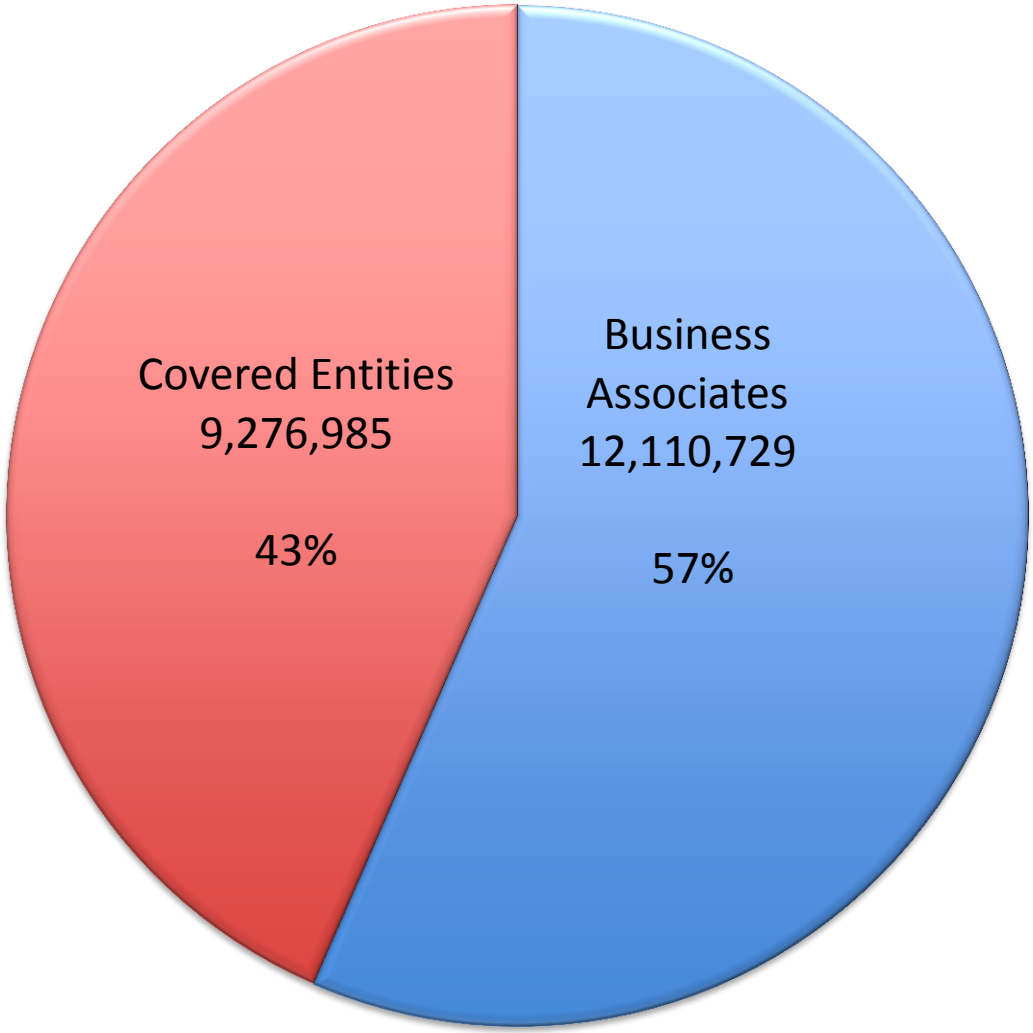



"Somehow your medical records got faxed to a complete stranger. He has no idea what's wrong with you either."

Business Associate Involvement
September 2009 - December 2012

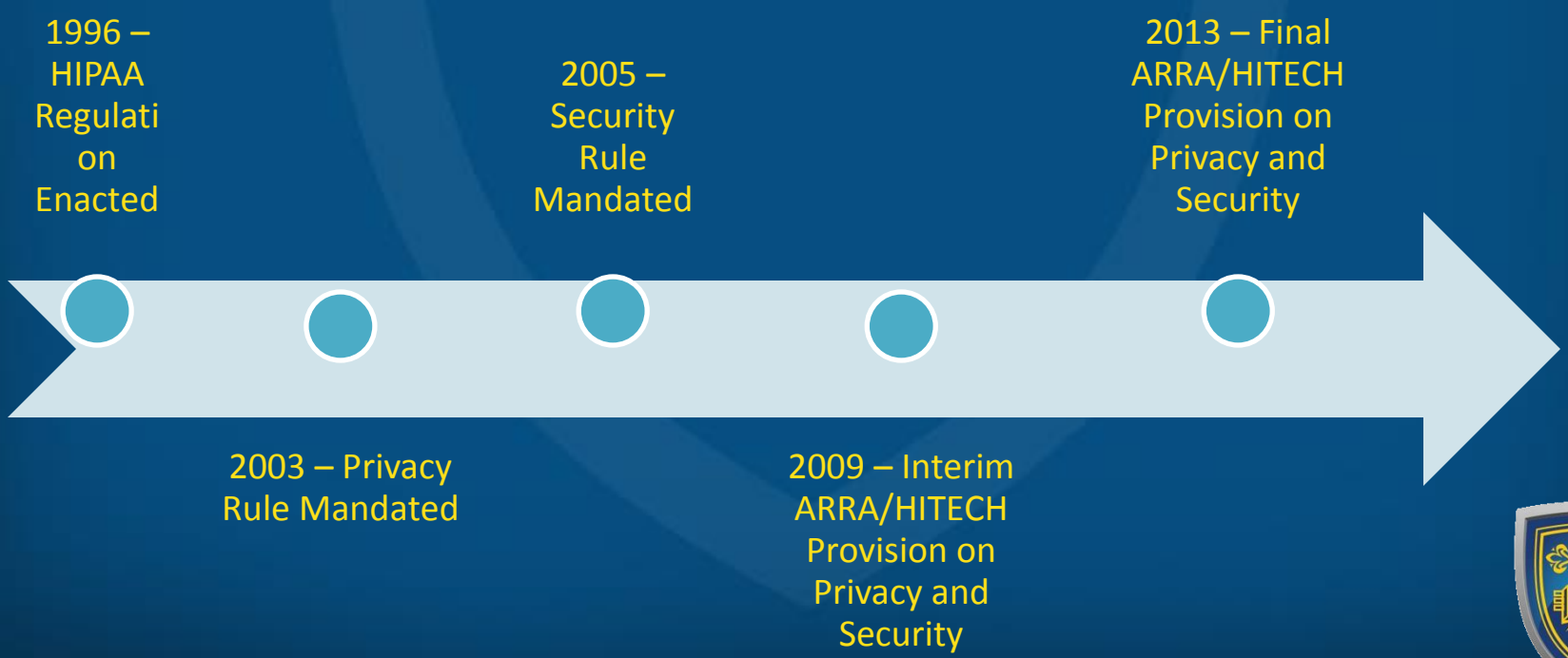


People Impacted By Breach
September 2009 - December 2012



Health Insurance Portability and Accountability Act (HIPAA) of 1996

First attempt at development of federal rules and regulations to protect the privacy and security of Protected Health Information (PHI)



Why the Heightened Focus on Privacy and Security?

- Amount and mobility of data
- Potential Harm: to patients and institutions
- Little enforcement of HIPAA
- EHR Incentive Program
- Because it is the RIGHT thing to do!

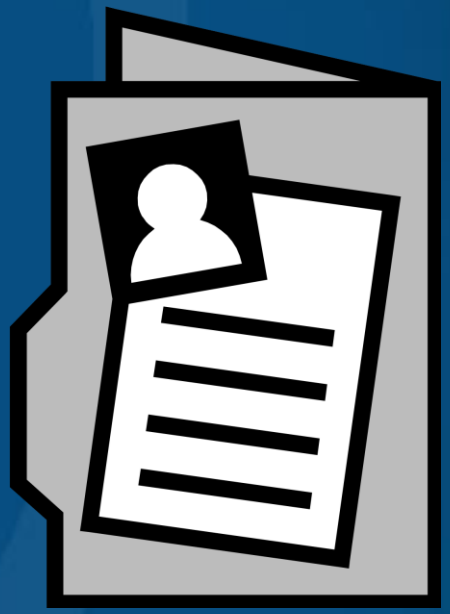

NANCY, I'M NOT SURE THAT'S WHAT HIPAA HAD IN MIND.

What is Protected Health Information?

- **Protected Health Information (PHI)**
  - Health information that identifies an individual, or could create a reasonable basis to believe the information could be used to identify an individual
  - Can be past, present, or future information
- **Electronic Protected Health Information (ePHI)**
  - Health Information that is transmitted or maintained in electronic format

Examples of Protected Health Information

- Patient's Name
- Age / Date of Birth
- Address
- Telephone Numbers
- Medical Record Number
- Social Security Number
- Account Number
- Health History or Conditions
- Treatment of Medications
- Dates of Treatments and Hospitalizations
- Hospital or Clinic Bill
- Biometric Identifiers



What are the Major HIPAA Compliance Areas?

Privacy Requirements

- Notices, Authorizations and Consents
- Accounting of Disclosures
- Business Associates
- Breach Notification

Security Requirements

- Physical , Technical and Administrative Safeguards
- Business Associates
- Risk Assessment and Compliance Programming
- Business Associate Changes
- Breach Notification
- Other Requirements

HIPAA – The Privacy Rule

- Published on December 28, 2000
- Final Rule published on August 14, 2002
- Effective Date – April 14, 2003

HIPAA – The Privacy Rule

The Final HIPAA Privacy Rule (45 CFR Parts 160 and 164) focused on three major purposes:

1. protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information;

2. to improve the quality of health care in the U.S. by restoring trust in the health care system, and

1. to improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals.

Minnesota Health Record Act

Minnesota Statutes 144.291 – 144.298

- Overall, HIPAA Law will be followed by Minnesota except in these situations where Minnesota is more strict:
  - Release of Information for the purpose of treatment
  - Disclosures to Law Enforcement
  - Research
  - Minnesota state law also defines how much to charge for records http://www.health.state.mn.us/divs/hpsc/dap/maxcharge.pdf

High Level Overview: Privacy Practices

- Appointment of Chief Privacy Officer
- Notice of Privacy Practices
- Disclosures
  - Minimum Necessary
  - Authorizations
  - Accounting of Disclosures (extended through ARRA IFR)
  - Request Restrictions on where PHI is sent
  - Designated Record Set
- Business Associate Agreements (extended through ARRA IFR)
- Revocation of Authorizations
- Medical Record Amendments
- Alternative forms of Communication with Patients
- Training of the Workforce
- Privacy/Breach Investigations and Notifications (extended through ARRA IFR)

HIPAA – The Security Rule

- Final Rule Published February 20, 2003
- Effective Date – April 20, 2005
- The Final HIPAA Security Rule defines administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic PHI.

Administrative Safeguards

Standards	Implementation Specifications	R = Required A = Addressable
Security Management Process	Risk Analysis	R
	Risk Management	R
	Sanction Policy	R
	Information System Activity Review	R
Assigned Security Responsibility	Designate Security Officer	R
Workforce Security	Authorization and/or Supervision	A
	Workforce Clearance Procedure	A
	Termination Procedures	A

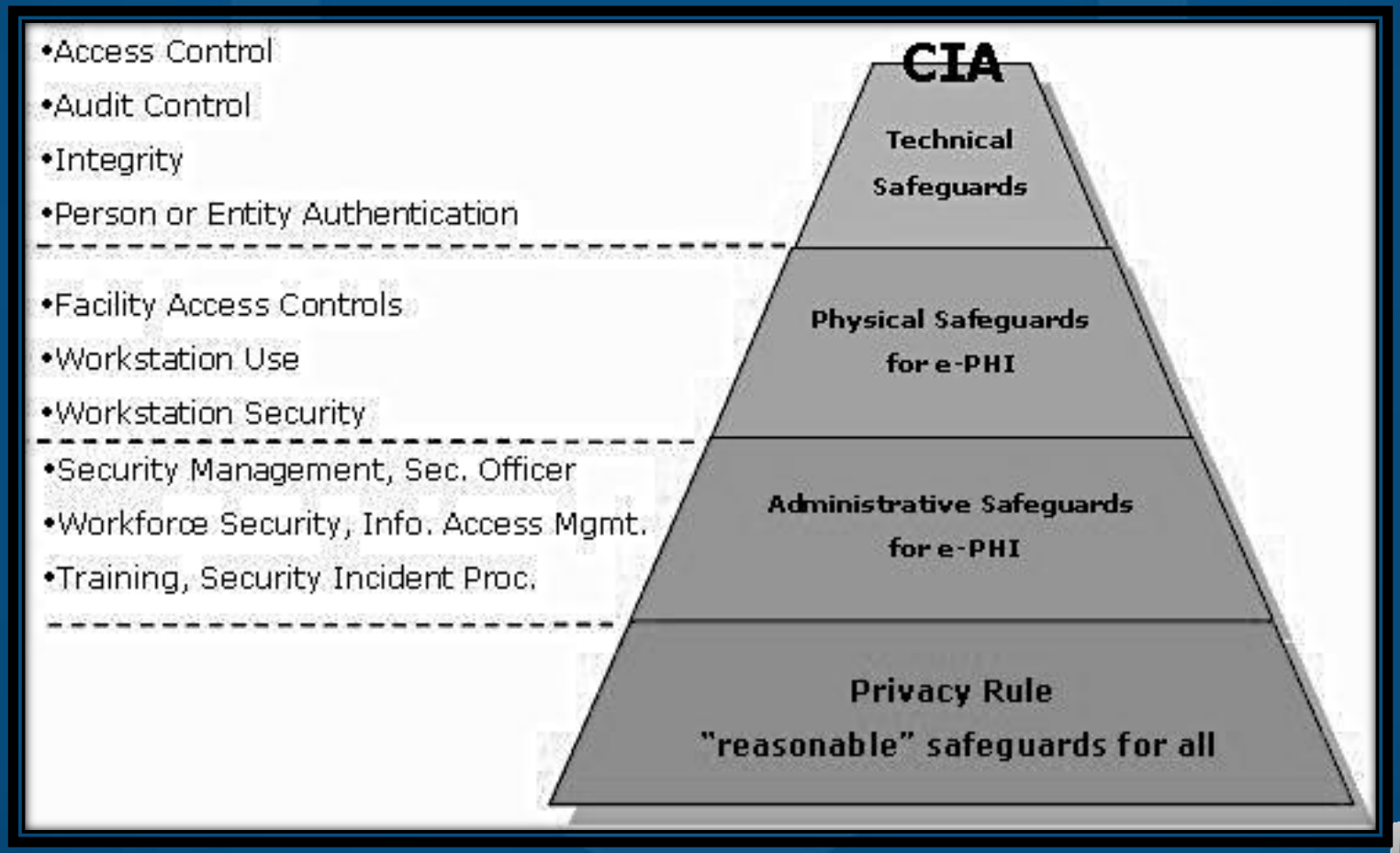
What's the Focus of the Security Rule

There are 4 distinct parts to the Security Rule:

1. Administrative Safeguards are administrative actions, including the establishment of policies and procedures, to manage the activities needed to establish security measures that protect ePHI.
2. Physical Safeguards are physical measures and policies and procedures, including policies and procedures, to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.
3. Technical Safeguards are the technology, including policies and procedures for its use, that protect ePHI and control access to it.
4. Organizational Safeguards are arrangements made between organizations to protect ePHI, including Business Associate Agreements.

One Size Does Not Fit All!!!

HIPAA and Confidentiality, Integrity, Accessibility (CIA)



Source: http://www.hipaaacademy.net/consulting/hipaaSecurityRuleOverview.html

Addressable v. Required

- **Standards are broken up into two categories (45 CRF 164.306(d))**
- **Addressable** – the covered entity must assess the reasonableness and appropriateness of the safeguard to protect the entity's ePHI
  - The size, complexity and capability of the covered entity
  - The covered entity technical infrastructure, hardware, and software security capabilities
  - The costs of security measures
  - The probability and criticality of potential risks to ePHI.

- **Required –** the covered entity must comply with the standard and implement policies and/or procedures that meet the requirement

American Recovery and Reinvestment Act (ARRA) of 2009

- February 2009, President Obama signed ARRA
- ARRA defines the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII
  - Strengthens HIPAA Privacy and Security Rules
  - Affects both Covered Entities and their Business Associates
  - Published draft privacy regulations on July 14, 2010 in the Federal Register
  - Responses to the draft regulations were due by September 13, 2010

HIPAA/HITECH Act Privacy, Security, Enforcement, and Breach Notification Modifications Final Rule - 2013

January 17, 2013 – Final Rule Announced

Friday, January 25, 2013 – Final Rule Published

The Final Rule Contains Modifications to

- The Breach Notification Rule.
- The HIPAA Enforcement Rule, implementing changes mandated by the HITECH Act.
- The Privacy and Security Rules, implementing changes mandated by the HITECH Act, as well as other changes to the Privacy Rule proposed in July 2010.
- The Privacy Rule, implementing changes required by the Genetic Information Nondiscrimination Act.

HITECH's New Fines and Civil Penalties

- Significant increase to the penalties for noncompliance of HIPAA's Privacy and Security Rules as well as HITECH provisions.

- New penalties are effective for violations that occur after February 17, 2009.

- There is no overall cap on civil monetary penalties under HITECH.

HITECH New Civil Penalties

- Under HIPAA, criminal penalties are defined as "wrongful disclosure of individually identifiable health information."
- The definition was enhanced to state that an individual may be subject to criminal penalties if a person knowingly obtains and discloses PHI in violation of HIPAA and/or the HITECH privacy and security provisions.
- Penalties are the following:

Tier	Fine	Imprisonment
Knowing Misuse	Up to $50,000	Up to 1 year
Knowing Misuse under false pretenses	Up to $100,000	Up to 5 years
Knowing Misuse with intent to sell, transfer, or use PHI for commercial advantage, personal gain or malicious intent	Up to $250,000	Up to 10 years

Recent Civil Penalties

Incident: A researcher at the UCLA School of Medicine received a notice of termination. In retaliation, that evening, he accessed the medical records of his superior and co-workers, and during three other periods over the next four weeks, he accessed UCLA patient records, many of them involving celebrities, a total of 323 times.
Penalty: The researcher was sentenced to four years in prison for violating the HIPAA Privacy Rule
The OCR is not the only enforcement agency taking action for HIPAA violations. Licensing boards and employers can also take action including suspension and termination.

Incident: A doctor and two hospital employees accessed the medical records of slain Arkansas TV reporter, Anne Pressly, who was found severely beaten in her home and died five days later. The details of her attack were leaked to the media.
Penalty: The three individuals pled guilty to misdemeanors for violating HIPAA Privacy Rules. A federal judge fined the doctor and the two hospital employees and sentenced them to one year probation. The hospital suspended the doctor's privileges for two weeks and terminated the two employees, an account representative and an emergency room coordinator.

Incident: A physician in Rhode Island posted details of some of her emergency room encounters on Facebook.
Penalty: The Rhode Island Board of Medical Licensure found her guilty of unprofessional conduct and issued a reprimand and a fine. Even though patient names were not used, there was sufficient information about the nature of the injuries to one patient to allow an unauthorized third party to figure out who the patient was. The physician claimed she did not intend to disclose confidential information.

Retrieved from: http://compliance.med.nyu.edu/news/documenting-inpatient-admissions

HITECH Fines for Breaches

Tiers	Per Violation Minimum	Per Violation Maximum	Max per Calendar Year per Violation
Tier A – "Did not know"	$100	$50,000	$1,500,000
Tier B – "Reasonable Cause"	$1,000	$50,000	$1,500,000
Tier C – "Willful Neglect – Corrected"	$10,000	$50,000	$1,500,000
Tier D – "Willful Neglect – Not Corrected"	$50,000	$1,500,000	$1,500,000

Recent Fines in the News

OCR Fines Alaska Medicaid $1.7 Million for HIPAA Violations

Written by Joseph Goedert, June 26, 2012, http://www.healthdatamanagement.com

"The Alaska Department of Health and Social Services will pay a $1.7 million federal fine to resolve violations of the HIPAA Security Rule under its Medicaid program. The agency also has agreed to a corrective action program negotiated with the federal HHS Office for Civil Rights. The action comes following the theft of a USB drive, from the vehicle of a DHSS employee, that may have contained protected health information, according to a statement from the OCR. An investigation found DHSS had failed on many levels to protect electronic PHI.…."

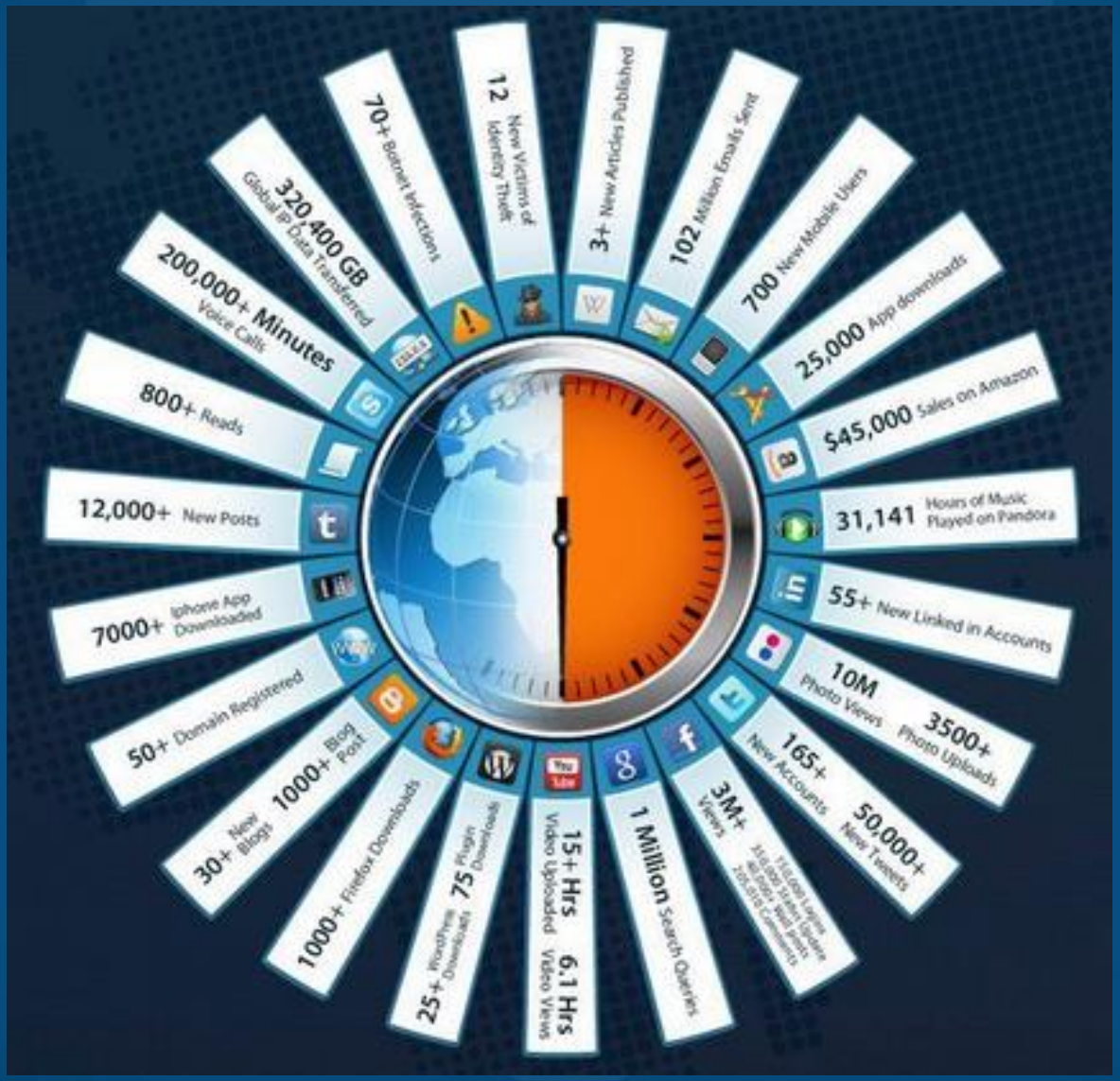
Massachusetts General Pays $1M to Settle HIPAA Violation Allegations

Written by Molly Gamble, February 24, 2011, http://www.beckershospitalreview.com

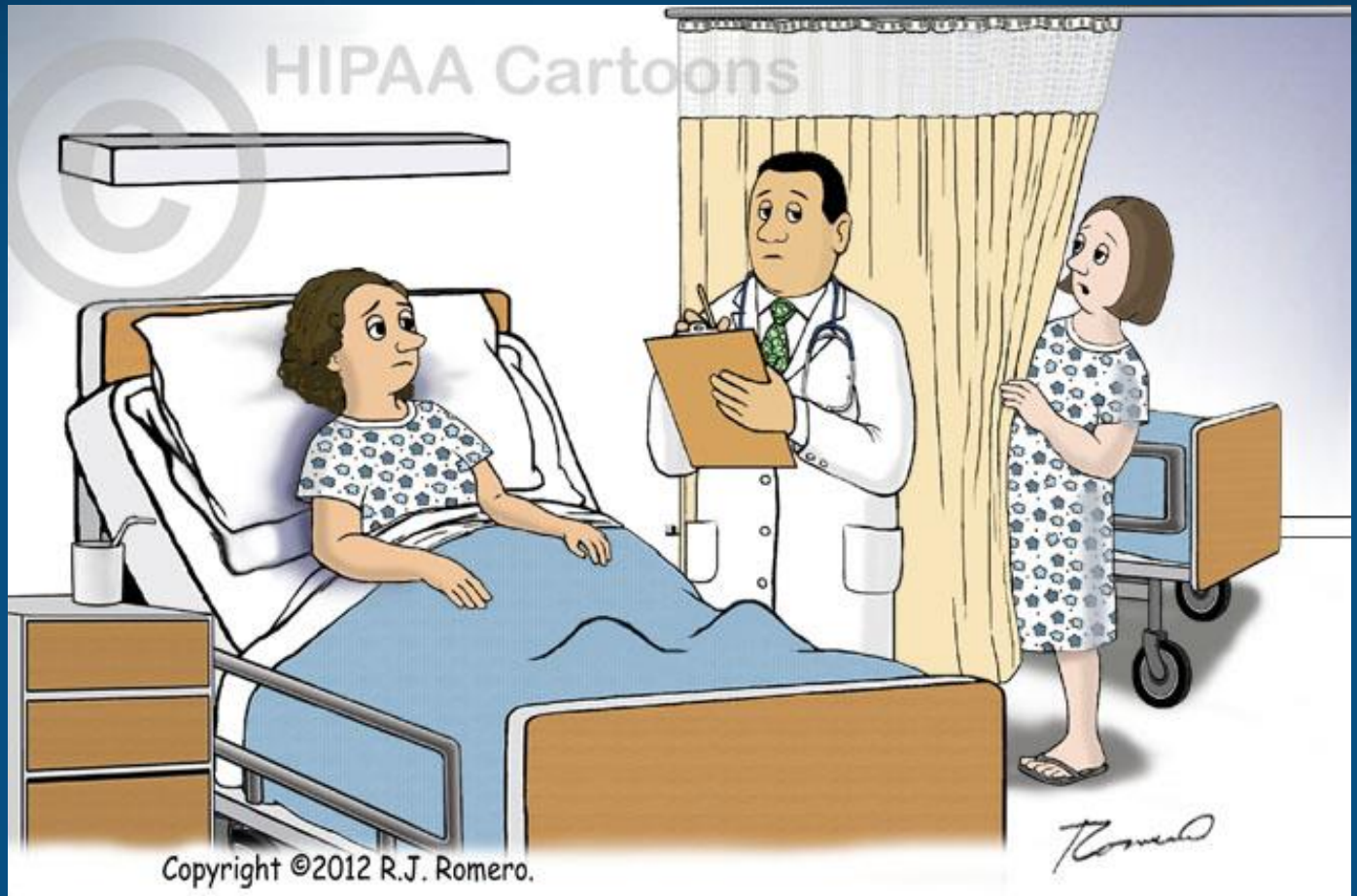
"The General Hospital Corporation and Massachusetts General Physicians Organization, representing Massachusetts General Hospital in Boston, has agreed to pay the U.S. government $1 million to settle allegations that the hospital system violated the HIPAA privacy rule, according to a news release from the U.S. Department of Health and Human Services…"

Social Networking – The Need to Control is Now

What Happens in 30 Seconds on the Web



Source: http://socialmedia4us.files.wordpress.com/2013/01/what-happens-on-the-web-in-30-seconds_jpg


HIPAA Cartoons
Copyright ©2012 R.J. Romero.
"Excuse me doctor, would you spell that medical term? I want to tell my Facebook friends all about the lady in the bed next to me."

Where do Meaningful Use and HIPAA Intersect?

Eligible Provider (EP) Core Measure #15 and Eligible Hospital (EH) and Critical Access Hospital (CAH) Core Objective #14

- **Objective**: Both of these measures require a EP, EH, or CAH to "protect health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities."
- **Measure**: This is measured by "**conducting** or reviewing 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."

Meaningful Use Stage 2

- The NPRM on Stage 2 Meaningful Use states ""We do not propose to change the HIPAA Security Rule requirements or require any more than would be required under HIPAA. We only emphasize the importance of an EP or hospital including in its security risk analysis an assessment of the reasonableness and appropriateness of encrypting electronic protected health information as a means of securing it, and where it is not reasonable and appropriate, the adoption of an equivalent alternative measure."
- The Risk Analysis and Management process MUST be completed for each year that the EH/CAH or EP attests for meaningful use

- Source: http://www.healthcareinfosecurity.com/articles.php?art_id=4533

Meaningful Use – Stage 2

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), including addressing the encryption/security of data at rest 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's risk management process.

Reference: Tom Walsh Consulting, LLC:
Risk Analysis Workshop

2014 EHR Certification Criteria

- The Major Changes to the Encryption requirements for Data at Rest

- The Certification Regulation is made up of 2 steps:
  - If EHR technology manages electronic health information on an end-user device and the electronic health information remains stored on the device after use of the EHR technology on that device has stopped, the electronic health information must be encrypted in accordance with the standard specified in § 170.210(a)(1). This capability must be enabled by default (i.e., turned on) and must only be permitted to be disabled (and re- enabled) by a limited set of identified users.
  - Electronic health information managed by EHR technology never remains stored on end-user devices after use of the EHR technology

Source: http://www.gpo.gov/fdsys/pkg/FR-2012-03-07/pdf/2012-4430.pdf

REACH Privacy and Security Work

- Risk Assessment Readiness Assessment
- Privacy and Security Bootcamps
- Education regarding Privacy and Security
- Burning Issues Radio Show
- Webinars

What Are Some General HIPAA Resources?

HealthSmart Privacy and Security E-Box, The College of St. Scholastica (bootcamp participants have full access)

U.S. Department of Health and Human Services

- http://www.hhs.gov/ocr/privacy/

HIPAA Collaborative of Wisconsin

- www.hipaacow.org

HITRC

- http://hitrc-collaborative.org/confluence/login.action;jsessionid=8F4F4460352F918A3565580E178EABD1?os_destination=%2Fdashboard.action

What Are Some General HIPAA Resources?

- ONC – P&S Page
  - http://healthit.hhs.gov/portal/server.pt?open=512&objID=1147&parentname=CommunityPage&parentid=8&mode=2&in_hi_userid=11673&cached=true
- OCR – Privacy and Security Page
  - http://www.hhs.gov/ocr/privacy/index.html
- ANSI
  - http://webstore.ansi.org/phi/

What Are Some General HIPAA Resources?

Miaoulis, W. M. (2011). Preparing for a HIPAA Security Compliance Assessment. Chicago: AHIMA

Dennis, J. (2010). Privacy: The Impact of ARRA, HITECH, and other Policy Initiatives. Chicago: AHIMA.

HIMSS Privacy and Security Toolkit

- http://www.himss.org/ASP/topics_PS_SmallProviders.asp

Information Security: Essential Guide to Healthcare Data Protection

- http://viewer.media.bitpipe.com/1152629439_931/1300215124_592/informationsecurity_e_guide_IThealth_v2.pdf

What Are Some General HIPAA Resources?

Krager,D and Krager, C. (2005). HIPAA for Medical Office Personnel. Thomson Delmar Learning

- http://www.hallrender.com/library/seminarTopics/ChangestoBusinessAssociate.pdf

“OCR Releases Accounting of Disclosure Proposed Rule.” American Health Information Management Association Advantage E-Alert. May 27, 2011.

- https://newsletters.ahima.org/newsletters/ealert/2011/05_27_11_special.html

References

- Borten, K (2009). *The HIPAA and HITECH Toolkit.*
- HIPAA Academy
  - http://www.hipaaacademy.net/consulting/hipaaSecurityRuleOverview.html
- HHS Health Information Privacy: Breach Notification Final Rule Update.
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/finalruleupdate.html
- Federal Register August 24, 2009. 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule
  - http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf
- HHS Health Information Privacy: Breach Notification Rule
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html
- HHS HIPAA Enforcement
  - http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html
- AHIMA E-Alert October 20 - OIG releases HIPAA compliance Target areas
  - https://newsletters.ahima.org/newsletters/ealert/2011/10_20_11.html