Security Risk Assessment for Small Practices: Tools and Case Studies

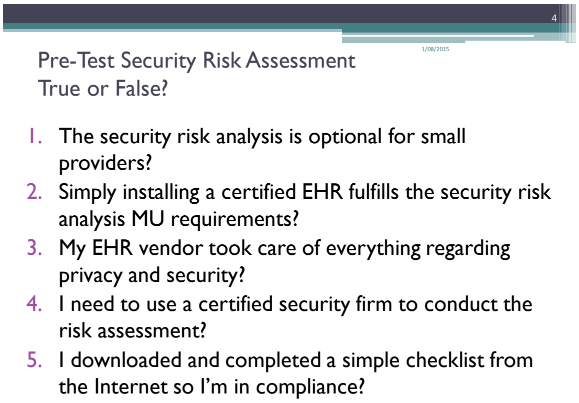
Joette Derricks, CMPE, CPC, CHC, CSSGB
September 7, 2015

Agenda

- Introduction to What Risks?
- What is a Security Risk Analysis?
- What Steps are Required for an Effective Risk Assessment?
- What Resources are Available to Help?
- Review Tools and Case Studies

Security Related Acronyms

CMS	Centers for Medicare & Medicaid Services
EHRs	Electronic Health Records
EPHI	Electronic Protected Health Information
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
MU	Meaningful Use
NIST	National Institute of Standards and Technology
OCR	Office of Civil Rights
ONC	Office of the National Coordinator for Health Information Technology
PHI	Protected Health Information

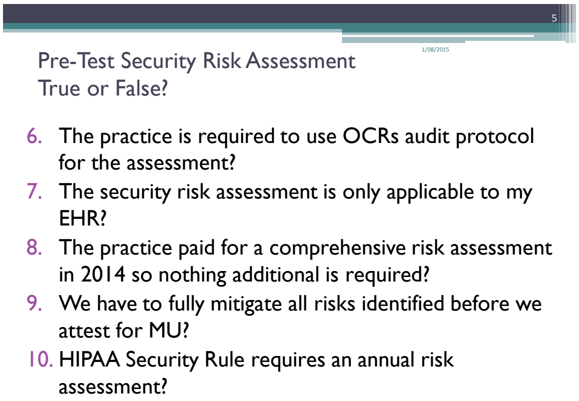


4

1/08/2015

Pre-Test Security Risk Assessment True or False?

1. The security risk analysis is optional for small providers?
2. Simply installing a certified EHR fulfills the security risk analysis MU requirements?
3. My EHR vendor took care of everything regarding privacy and security?
4. I need to use a certified security firm to conduct the risk assessment?
5. I downloaded and completed a simple checklist from the Internet so I'm in compliance?

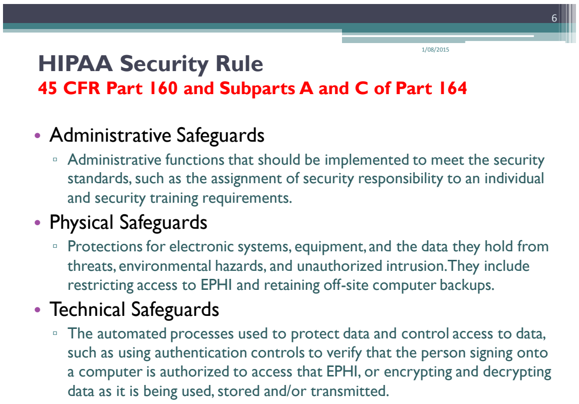


5

1/08/2015

Pre-Test Security Risk Assessment True or False?

6. The practice is required to use OCRs audit protocol for the assessment?
7. The security risk assessment is only applicable to my EHR?
8. The practice paid for a comprehensive risk assessment in 2014 so nothing additional is required?
9. We have to fully mitigate all risks identified before we attest for MU?
10. HIPAA Security Rule requires an annual risk assessment?

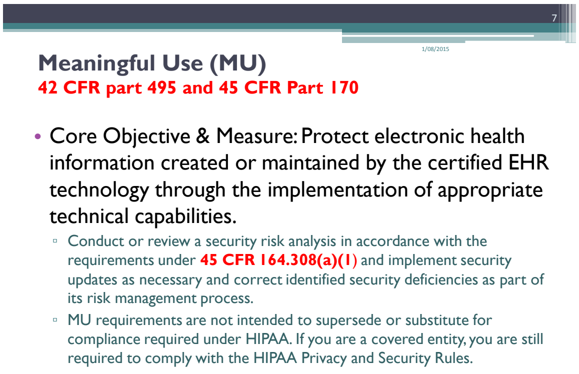


6

1/08/2015

HIPAA Security Rule
45 CFR Part 160 and Subparts A and C of Part 164

- Administrative Safeguards
  - Administrative functions that should be implemented to meet the security standards, such as the assignment of security responsibility to an individual and security training requirements.
- Physical Safeguards
  - Protections for electronic systems, equipment, and the data they hold from threats, environmental hazards, and unauthorized intrusion. They include restricting access to EPHI and retaining off-site computer backups.
- Technical Safeguards
  - The automated processes used to protect data and control access to data, such as using authentication controls to verify that the person signing onto a computer is authorized to access that EPHI, or encrypting and decrypting data as it is being used, stored and/or transmitted.

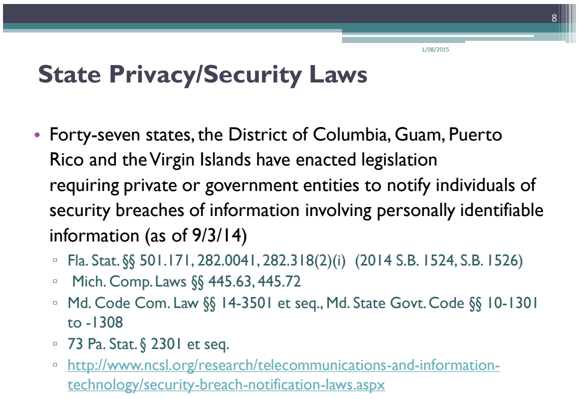


7

1/08/2015

Meaningful Use (MU)
42 CFR part 495 and 45 CFR Part 170

- Core Objective & Measure: Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.
  - 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.
  - MU requirements are not intended to supersede or substitute for compliance required under HIPAA. If you are a covered entity, you are still required to comply with the HIPAA Privacy and Security Rules.

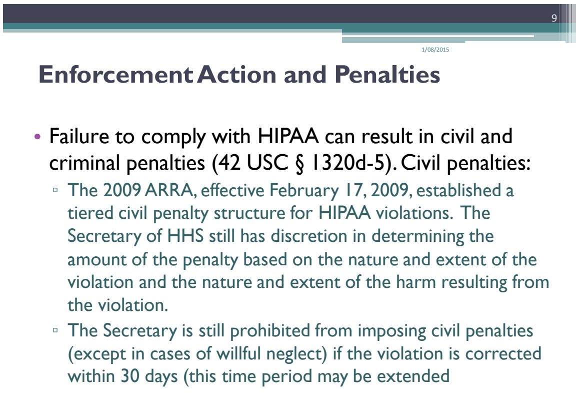


8

1/08/2015

State Privacy/Security Laws

- Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information (as of 9/3/14)
  - Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i) (2014 S.B. 1524, S.B. 1526)
  - Mich. Comp. Laws §§ 445.63, 445.72
  - Md. Code Com. Law §§ 14-3501 et seq., Md. State Govt. Code §§ 10-1301 to -1308
  - 73 Pa. Stat. § 2301 et seq.
  - http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx



9

1/08/2015

Enforcement Action and Penalties

- Failure to comply with HIPAA can result in civil and criminal penalties (42 USC § 1320d-5). Civil penalties:
  - The 2009 ARRA, effective February 17, 2009, established a tiered civil penalty structure for HIPAA violations. The Secretary of HHS still has discretion in determining the amount of the penalty based on the nature and extent of the violation and the nature and extent of the harm resulting from the violation.
  - The Secretary is still prohibited from imposing civil penalties (except in cases of willful neglect) if the violation is corrected within 30 days (this time period may be extended

10

1/08/2015

HIPAA Violation	Minimum Penalty	Maximum Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to willful neglect but violation is corrected within the required time period	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation is due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

11

1/08/2015

Enforcement Action and Penalties - Civil

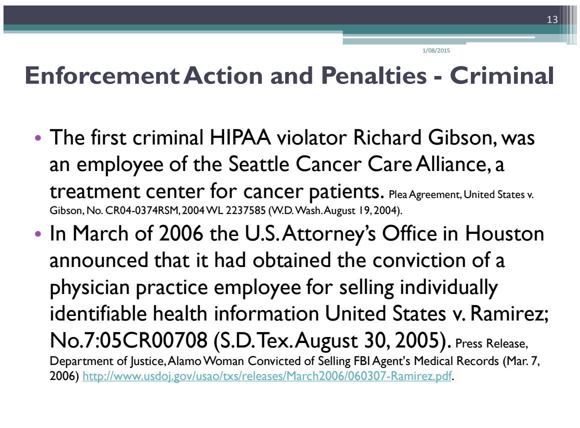
- UCLA paid $865,500—employees repeatedly looked at EPHI of two celebrity patients
- BCBS Tennessee paid $1,500,000—57 unencrypted computer hard drives were stolen with EPHI of over 1 million individuals
- New York-Presbyterian Hospital and Columbia University were fined a total of $4.8 million for lack of safeguards regarding EPHI
- OCR pilot audit program results; security deficiencies accounted for 60% of the findings and observation
- http://www.hhs.gov/ocr/privacy/index.html

12

1/08/2015

Enforcement Action and Penalties - Criminal

- In June 2005, the U.S. Department of Justice (DOJ) clarified who can be held criminally liable under HIPAA. Covered entities and specified individuals whom "knowingly" obtain or disclose individually identifiable health information in violation of the Administrative Simplification Regulations face a fine of up to $50,000, as well as imprisonment up to one year.
- Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to five years in prison.
- Finally, offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000, and imprisonment for up to ten years.

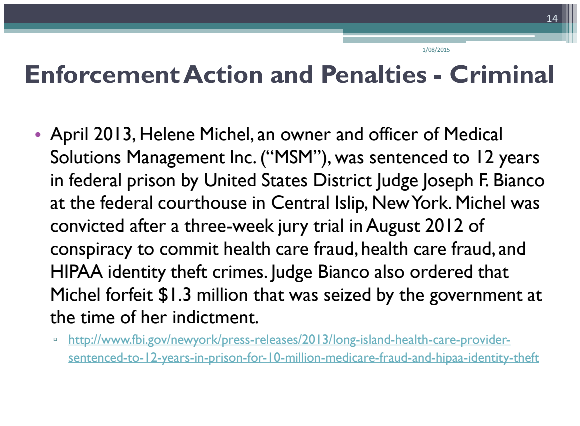


13

1/08/2015

Enforcement Action and Penalties - Criminal

- The first criminal HIPAA violator Richard Gibson, was an employee of the Seattle Cancer Care Alliance, a treatment center for cancer patients. Plea Agreement, United States v. Gibson, No. CR04-0374RSM, 2004 WL 2237585 (W.D. Wash. August 19, 2004).
- In March of 2006 the U.S. Attorney's Office in Houston announced that it had obtained the conviction of a physician practice employee for selling individually identifiable health information United States v. Ramirez; No.7:05CR00708 (S.D. Tex. August 30, 2005). Press Release, Department of Justice, Alamo Woman Convicted of Selling FBI Agent's Medical Records (Mar. 7, 2006) http://www.usdoj.gov/usao/txs/releases/March2006/060307-Ramirez.pdf.

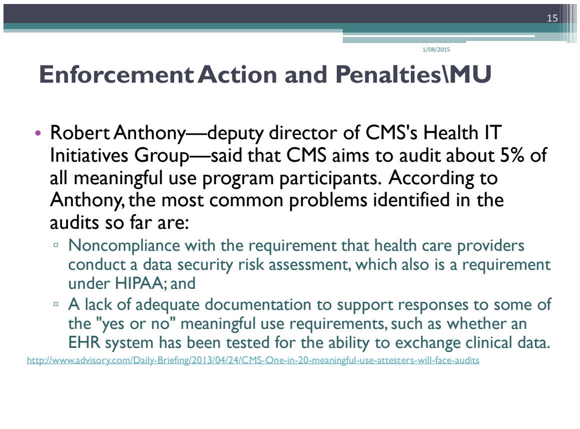


14

1/08/2015

Enforcement Action and Penalties - Criminal

- April 2013, Helene Michel, an owner and officer of Medical Solutions Management Inc. ("MSM"), was sentenced to 12 years in federal prison by United States District Judge Joseph F. Bianco at the federal courthouse in Central Islip, New York. Michel was convicted after a three-week jury trial in August 2012 of conspiracy to commit health care fraud, health care fraud, and HIPAA identity theft crimes. Judge Bianco also ordered that Michel forfeit $1.3 million that was seized by the government at the time of her indictment.
  - http://www.fbi.gov/newyork/press-releases/2013/long-island-health-care-provider-sentenced-to-12-years-in-prison-for-10-million-medicare-fraud-and-hipaa-identity-theft



15

1/08/2015

Enforcement Action and Penalties\MU

- Robert Anthony—deputy director of CMS's Health IT Initiatives Group—said that CMS aims to audit about 5% of all meaningful use program participants. According to Anthony, the most common problems identified in the audits so far are:
  - Noncompliance with the requirement that health care providers conduct a data security risk assessment, which also is a requirement under HIPAA; and
  - A lack of adequate documentation to support responses to some of the "yes or no" meaningful use requirements, such as whether an EHR system has been tested for the ability to exchange clinical data.

http://www.advisory.com/Daily-Briefing/2013/04/24/CMS-One-in-20-meaningful-use-attesters-will-face-audits

16

1/08/2015

Enforcement Action and Penalties\MU

- The letter the hospital received said it all, "Based on our desk review of the supporting documentation furnished by the facility, we have determined that Hospital X has not met the meaningful use criteria… Since your facility did not meet the meaningful use criteria, the EHR incentive payment will be recouped. You will receive a demand for your total Medicare EHR incentive payment shortly from the EHR HITECH Incentive Payment Center."

17

1/08/2015

Security Risk Assessment

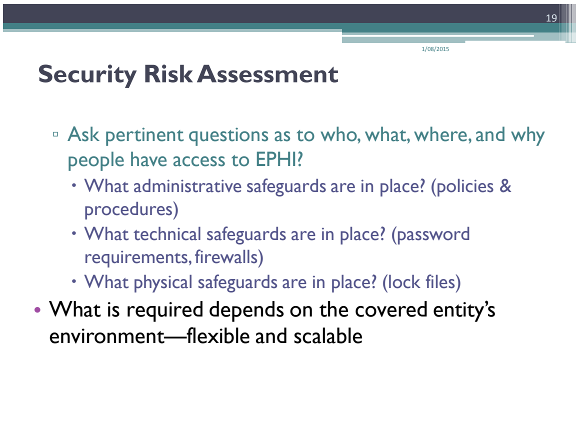
- **Risk Analysis --**Conduct an accurate and *thorough* assessment of the potential *risks* and *vulnerabilities* to the **confidentiality, integrity, and availability** of ePHI *held* by the organization.
- **Risk Management --**Implement security measures *sufficient* to reduce risks and vulnerabilities to a *reasonable and appropriate* level to comply.

18

1/08/2015

Security Risk Assessment

- **Confidentiality**—EPHI is not made available or disclosed to unauthorized persons or processes
- **Integrity**—EPHI has not, can not be altered or destroyed in an unauthorized manner
- **Availability**—EPHI is accessible and useable upon demand by an authorized person

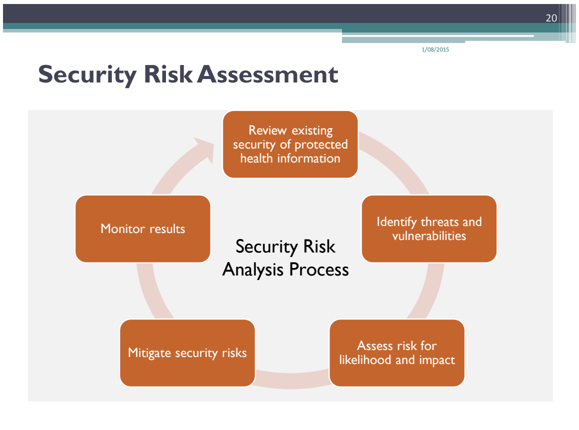


19

1/08/2015

Security Risk Assessment

- Ask pertinent questions as to who, what, where, and why people have access to EPHI?
  - What administrative safeguards are in place? (policies & procedures)
  - What technical safeguards are in place? (password requirements, firewalls)
  - What physical safeguards are in place? (lock files)
- What is required depends on the covered entity's environment—flexible and scalable

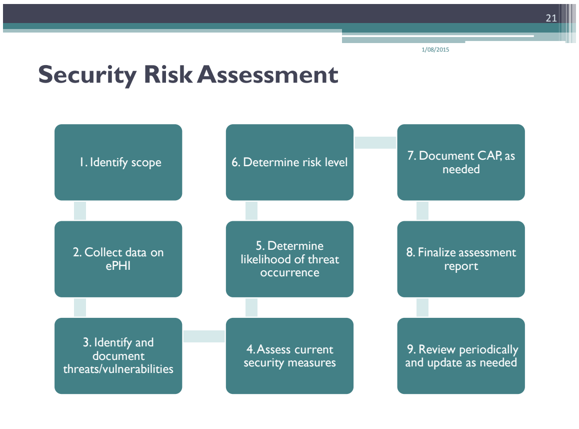


20

1/08/2015

Security Risk Assessment

Review existing security of protected health information
Identify threats and vulnerabilities
Assess risk for likelihood and impact
Mitigate security risks
Monitor results
Security Risk Analysis Process

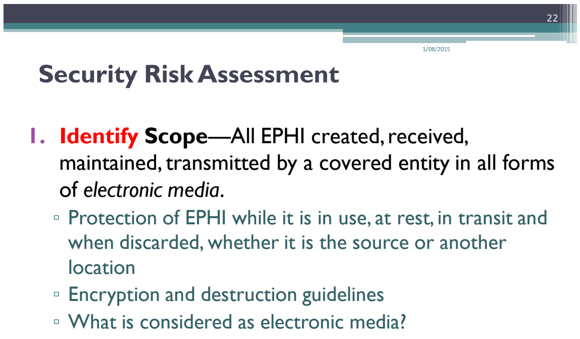


21

1/08/2015

Security Risk Assessment

1. Identify scope
2. Collect data on ePHI
3. Identify and document threats/vulnerabilities
4. Assess current security measures
5. Determine likelihood of threat occurrence
6. Determine risk level
7. Document CAP, as needed
8. Finalize assessment report
9. Review periodically and update as needed

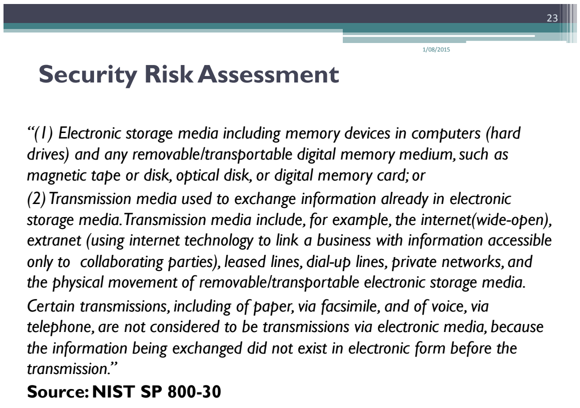


22

1/08/2015

Security Risk Assessment

1. **Identify Scope**—All EPHI created, received, maintained, transmitted by a covered entity in all forms of *electronic media*.
   - Protection of EPHI while it is in use, at rest, in transit and when discarded, whether it is the source or another location
   - Encryption and destruction guidelines
   - What is considered as electronic media?



23

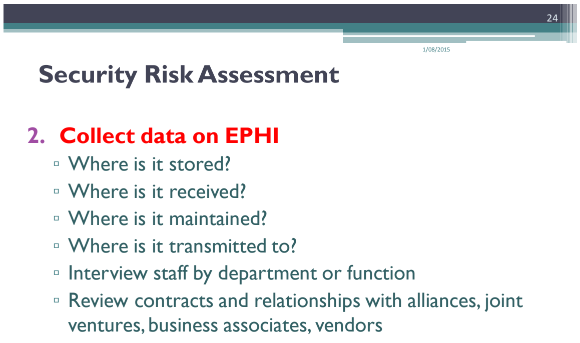
1/08/2015

Security Risk Assessment

"(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet(wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission."

Source: NIST SP 800-30

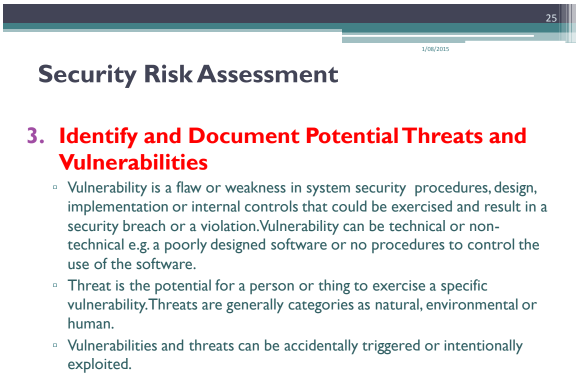


24

1/08/2015

Security Risk Assessment

2. **Collect data on EPHI**
   - Where is it stored?
   - Where is it received?
   - Where is it maintained?
   - Where is it transmitted to?
   - Interview staff by department or function
   - Review contracts and relationships with alliances, joint ventures, business associates, vendors

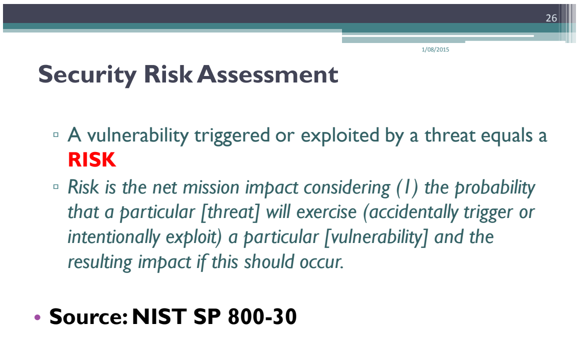


25

1/08/2015

Security Risk Assessment

3. **Identify and Document Potential Threats and Vulnerabilities**
   - Vulnerability is a flaw or weakness in system security procedures, design, implementation or internal controls that could be exercised and result in a security breach or a violation.Vulnerability can be technical or non-technical e.g. a poorly designed software or no procedures to control the use of the software.
   - Threat is the potential for a person or thing to exercise a specific vulnerability.Threats are generally categories as natural, environmental or human.
   - Vulnerabilities and threats can be accidentally triggered or intentionally exploited.



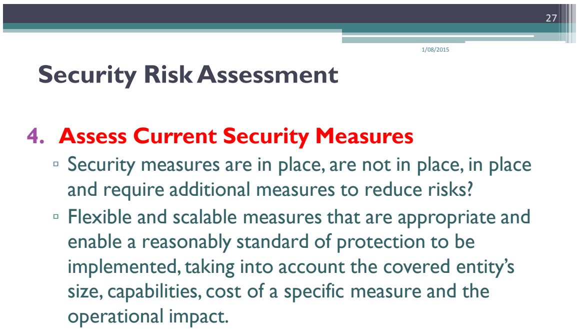
26

1/08/2015

Security Risk Assessment

- A vulnerability triggered or exploited by a threat equals a **RISK**
- *Risk is the net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and the resulting impact if this should occur.*

- **Source: NIST SP 800-30**

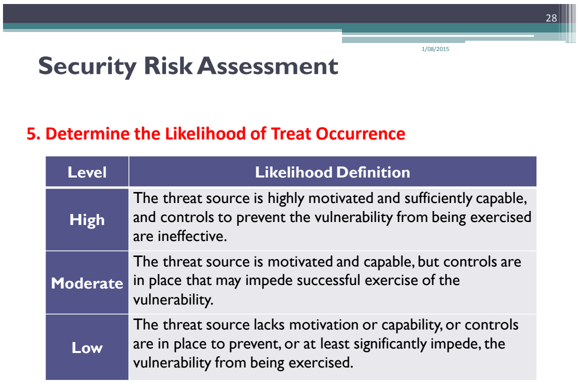


27

1/08/2015

Security Risk Assessment

4. **Assess Current Security Measures**
   - Security measures are in place, are not in place, in place and require additional measures to reduce risks?
   - Flexible and scalable measures that are appropriate and enable a reasonably standard of protection to be implemented, taking into account the covered entity's size, capabilities, cost of a specific measure and the operational impact.



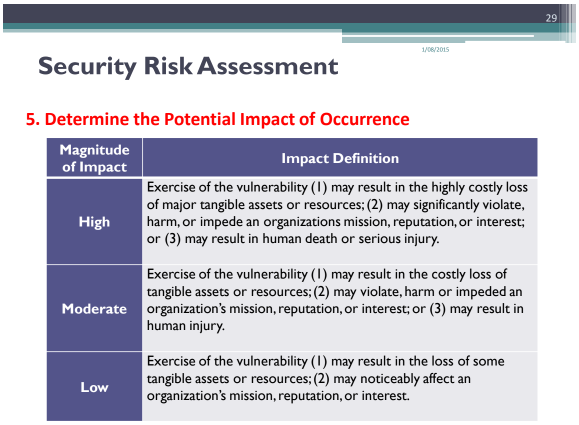
28

1/08/2015

Security Risk Assessment

5. Determine the Likelihood of Treat Occurrence

Level	Likelihood Definition
High	The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Moderate	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.



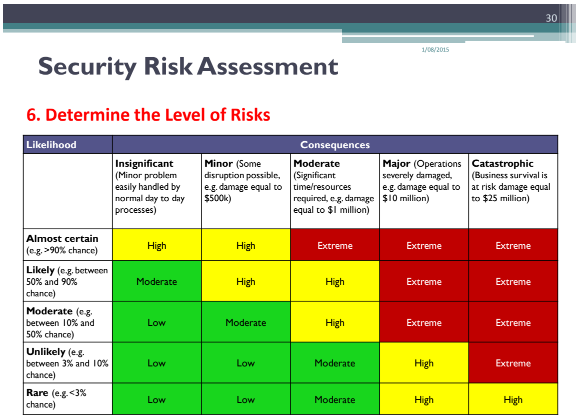
29

1/08/2015

Security Risk Assessment

5. Determine the Potential Impact of Occurrence

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organizations mission, reputation, or interest; or (3) may result in human death or serious injury.
Moderate	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm or impeded an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources; (2) may noticeably affect an organization's mission, reputation, or interest.



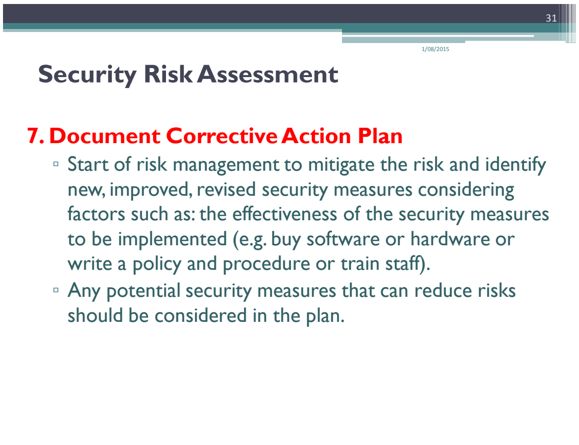
30

1/08/2015

Security Risk Assessment

6. Determine the Level of Risks

Likelihood	Consequences				
	Insignificant (Minor problem easily handled by normal day to day processes)	**Minor** (Some disruption possible, e.g. damage equal to $500k)	**Moderate** (Significant time/resources required, e.g. damage equal to $1 million)	**Major** (Operations severely damaged, e.g. damage equal to $10 million)	**Catastrophic** (Business survival is at risk damage equal to $25 million)
Almost certain (e.g. >90% chance)	High	High	Extreme	Extreme	Extreme
Likely (e.g. between 50% and 90% chance)	Moderate	High	High	Extreme	Extreme
Moderate (e.g. between 10% and 50% chance)	Low	Moderate	High	Extreme	Extreme
Unlikely (e.g. between 3% and 10% chance)	Low	Low	Moderate	High	Extreme
Rare (e.g. <3% chance)	Low	Low	Moderate	High	High



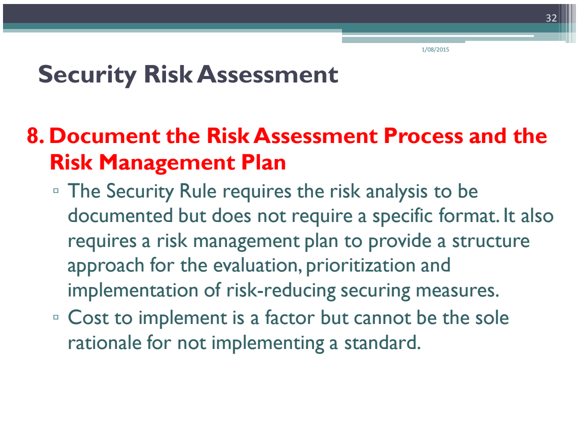
31

1/08/2015

Security Risk Assessment

7. Document Corrective Action Plan

- Start of risk management to mitigate the risk and identify new, improved, revised security measures considering factors such as: the effectiveness of the security measures to be implemented (e.g. buy software or hardware or write a policy and procedure or train staff).
- Any potential security measures that can reduce risks should be considered in the plan.



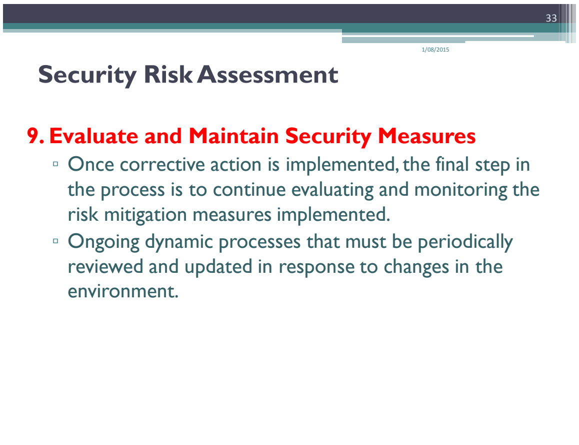
32

1/08/2015

Security Risk Assessment

8. Document the Risk Assessment Process and the Risk Management Plan

- The Security Rule requires the risk analysis to be documented but does not require a specific format. It also requires a risk management plan to provide a structure approach for the evaluation, prioritization and implementation of risk-reducing securing measures.
- Cost to implement is a factor but cannot be the sole rationale for not implementing a standard.



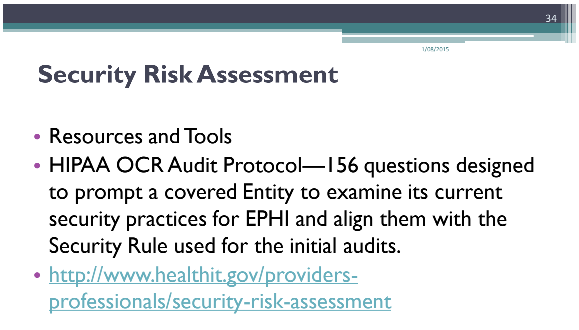
33

1/08/2015

Security Risk Assessment

9. Evaluate and Maintain Security Measures

- Once corrective action is implemented, the final step in the process is to continue evaluating and monitoring the risk mitigation measures implemented.
- Ongoing dynamic processes that must be periodically reviewed and updated in response to changes in the environment.

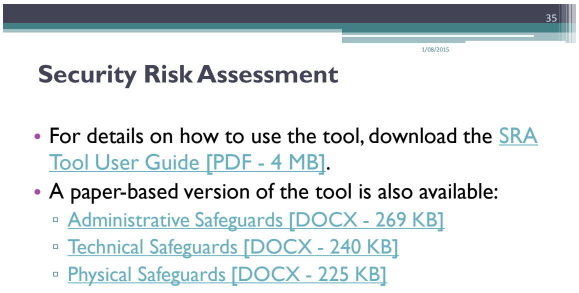


34

1/08/2015

Security Risk Assessment

- Resources and Tools
- HIPAA OCR Audit Protocol—156 questions designed to prompt a covered Entity to examine its current security practices for EPHI and align them with the Security Rule used for the initial audits.
- http://www.healthit.gov/providers-professionals/security-risk-assessment

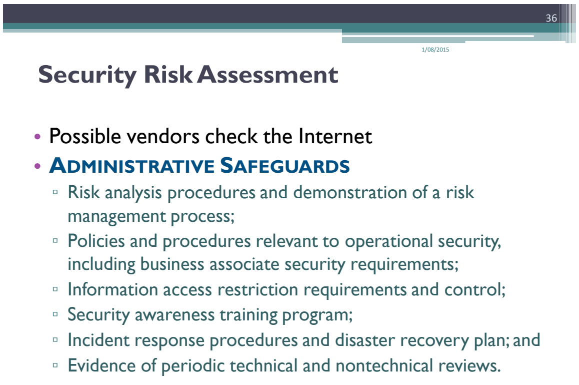


35

1/08/2015

Security Risk Assessment

- For details on how to use the tool, download the SRA Tool User Guide [PDF - 4 MB].
- A paper-based version of the tool is also available:
  - Administrative Safeguards [DOCX - 269 KB]
  - Technical Safeguards [DOCX - 240 KB]
  - Physical Safeguards [DOCX - 225 KB]

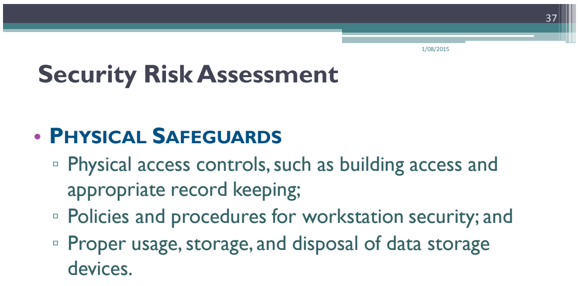


36

1/08/2015

Security Risk Assessment

- Possible vendors check the Internet
- **Administrative Safeguards**
  - Risk analysis procedures and demonstration of a risk management process;
  - Policies and procedures relevant to operational security, including business associate security requirements;
  - Information access restriction requirements and control;
  - Security awareness training program;
  - Incident response procedures and disaster recovery plan; and
  - Evidence of periodic technical and nontechnical reviews.

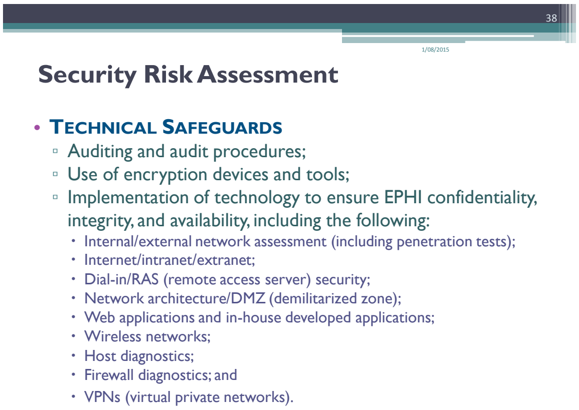


37

1/08/2015

Security Risk Assessment

- **Physical Safeguards**
  - Physical access controls, such as building access and appropriate record keeping;
  - Policies and procedures for workstation security; and
  - Proper usage, storage, and disposal of data storage devices.

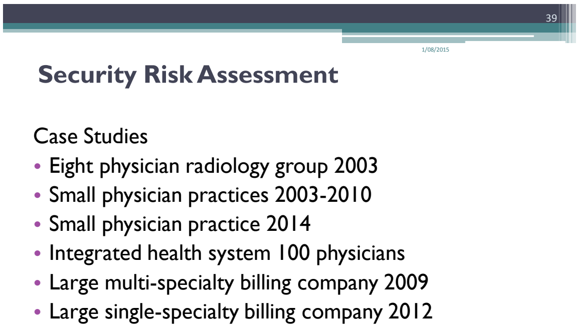


38

1/08/2015

Security Risk Assessment

- **Technical Safeguards**
  - Auditing and audit procedures;
  - Use of encryption devices and tools;
  - Implementation of technology to ensure EPHI confidentiality, integrity, and availability, including the following:
    - Internal/external network assessment (including penetration tests);
    - Internet/intranet/extranet;
    - Dial-in/RAS (remote access server) security;
    - Network architecture/DMZ (demilitarized zone);
    - Web applications and in-house developed applications;
    - Wireless networks;
    - Host diagnostics;
    - Firewall diagnostics; and
    - VPNs (virtual private networks).



39

1/08/2015

Security Risk Assessment

Case Studies

- Eight physician radiology group 2003
- Small physician practices 2003-2010
- Small physician practice 2014
- Integrated health system 100 physicians
- Large multi-specialty billing company 2009
- Large single-specialty billing company 2012

40

1/08/2015

Case Studies

1. Eight physician radiology group located in Southeastern Pennsylvania with imaging
   - Full set of privacy and security policies and procedures first drafted in 2002, and 2003 based on the HIPAA regulations
   - Security audit in 2004 + 2005 (using a checklist format with to do list), 2007 (re-write the polices and procedures and a complete re-assignment due to major expansion effort of physicians, employees, and facility)
   - Security training initially in 2003, and each year there after

41

1/08/2015

Case Studies

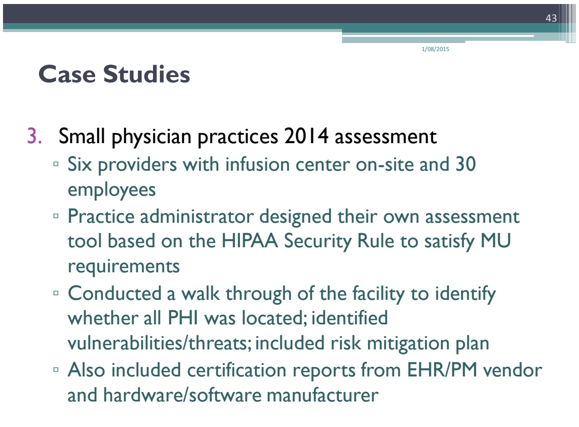
- Prompted by "loss" of two laptops and vandalism to medical record room
- Risk analysis included interviews, walk through, and questionnaires with physicians, supervisors and random employees
- Coordinated with internal IT coordinator and practice attorney – biweekly meetings with executive board
- Two months from start to finish
- Identified numerous deficiencies which board approved a two year mitigation process estimated at about $265, 000 cost of hardware/software upgrades and facility upgrades
- Continues to take security and all regulations seriously

42

1/08/2015

Case Studies

2. Small physician practices 2003-2010
   - Performed about 30 privacy and security risk assessments for clients with between three and twenty providers using the same basic format
   - Comprehensive package including assessment and CAP report, policies and procedures and training; average fee $10,000
   - Most common deficiencies were password sharing and loss of dictation tapes and/or backup tapes

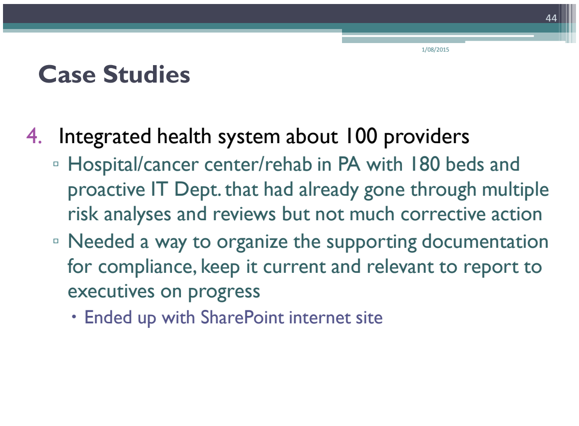


43

1/08/2015

Case Studies

3. Small physician practices 2014 assessment
   - Six providers with infusion center on-site and 30 employees
   - Practice administrator designed their own assessment tool based on the HIPAA Security Rule to satisfy MU requirements
   - Conducted a walk through of the facility to identify whether all PHI was located; identified vulnerabilities/threats; included risk mitigation plan
   - Also included certification reports from EHR/PM vendor and hardware/software manufacturer

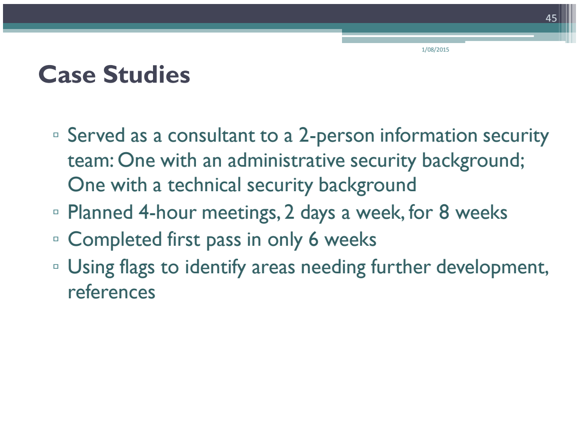


44

1/08/2015

Case Studies

4. Integrated health system about 100 providers
   - Hospital/cancer center/rehab in PA with 180 beds and proactive IT Dept. that had already gone through multiple risk analyses and reviews but not much corrective action
   - Needed a way to organize the supporting documentation for compliance, keep it current and relevant to report to executives on progress
     - Ended up with SharePoint internet site

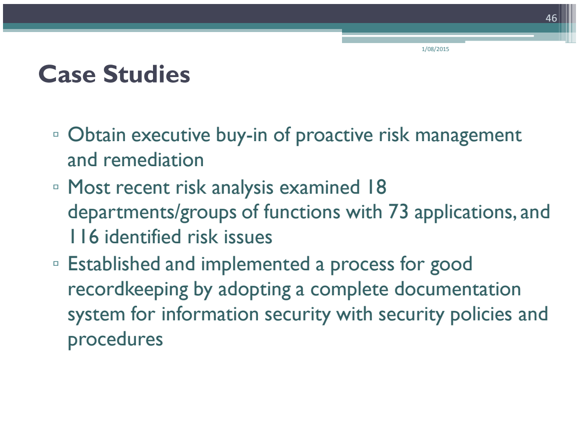


45

1/08/2015

Case Studies

- Served as a consultant to a 2-person information security team: One with an administrative security background; One with a technical security background
- Planned 4-hour meetings, 2 days a week, for 8 weeks
- Completed first pass in only 6 weeks
- Using flags to identify areas needing further development, references

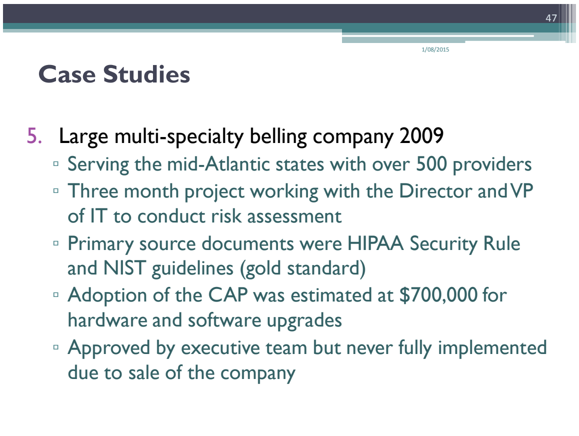


46

1/08/2015

Case Studies

- Obtain executive buy-in of proactive risk management and remediation
- Most recent risk analysis examined 18 departments/groups of functions with 73 applications, and 116 identified risk issues
- Established and implemented a process for good recordkeeping by adopting a complete documentation system for information security with security policies and procedures

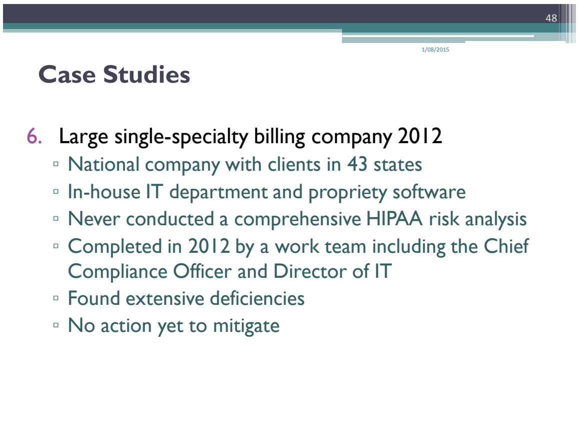


47

1/08/2015

Case Studies

5. Large multi-specialty belling company 2009
   - Serving the mid-Atlantic states with over 500 providers
   - Three month project working with the Director and VP of IT to conduct risk assessment
   - Primary source documents were HIPAA Security Rule and NIST guidelines (gold standard)
   - Adoption of the CAP was estimated at $700,000 for hardware and software upgrades
   - Approved by executive team but never fully implemented due to sale of the company



48

1/08/2015

Case Studies

6. Large single-specialty billing company 2012
   - National company with clients in 43 states
   - In-house IT department and propriety software
   - Never conducted a comprehensive HIPAA risk analysis
   - Completed in 2012 by a work team including the Chief Compliance Officer and Director of IT
   - Found extensive deficiencies
   - No action yet to mitigate

49

1/08/2015

Questions

Joette P. Derricks, MPA, CHC, CPC, CMPE, CSSGB
Derricks Consulting
jpderricks@gmail.com
(717)877-5416