HIPAA Security: How to Effectively Work With Attorneys and Consultants

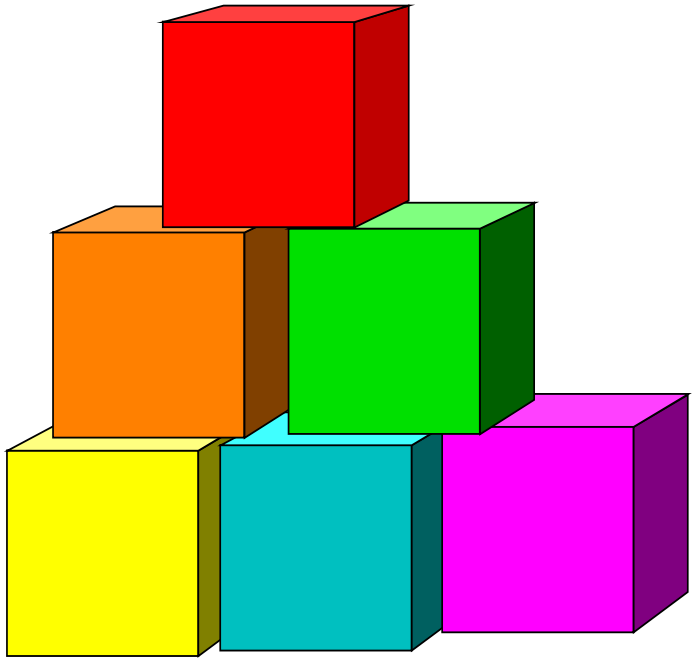
By: Andrew B. Wachler, Esq.
Wachler & Associates, P.C.
And
John C. Parmigiani
John C. Parmigiani & Associates, LLC

Overview

- Introduction and Background
  - Legal
  - Consultant

Security Primer Overview

- Confidentiality
- Integrity
- Availability



Security Primer Overview

- Standards are in 3 categories: administrative, physical, and technological
- Implementation specifications are “instructions” for compliance with standards and are either “required” or “addressable”

Security Primer Overview

- Question: to what extent will Security Rule be used to set standard of care for:
  - administrative
  - technological and
  - physical safeguards

  under the Privacy Rule

Security Primer Overview

- Documentation of thorough risk analysis is key to making informed judgment calls with respect to which specific technologies and security measures to implement

- May take into account: size; complexity and capabilities; technical infrastructure, hardware, software, and existing security capabilities; the costs of security measures; and the probability and criticality of potential risks to electronic PHI

Good Security Practices

- Access Controls- restrict user access to PHI based on need-to-know
- Authentication- verify identity and allow access to PHI by only authorized users
- Audit Controls- identify who did what and when relative to PHI
- ***Any enforcement of the regulation will focus on how well your organization is doing these!***

Security Truisms

- There is no such thing as 100% security
- Security is a business process- it is an investment, not an expense
- It is difficult to calculate the return on investment for security
- Threats and risks are constantly changing- you must know your real risks and determine the probability and impact of their occurrence
- Prioritize your security efforts and manage risks to a level acceptable to the organization

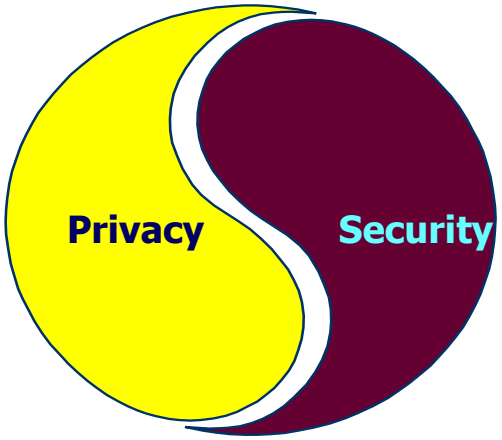
So…Security is Good Business

- "Reasonable measures" need to be taken to protect confidential information (due diligence)
- A balanced security approach provides due diligence without impeding health care
- Good security can reduce liabilities- patient safety, fines, lawsuits, bad public relations
- Security is essential to privacy

Without good security your organization will not be able to effectively exist in an emerging e-Health environment!

Serendipity Effect of Privacy Compliance

- Security and Privacy are inextricably linked
  - Can have Security by itself *but* cannot have Privacy without Security
  - Privacy has already necessitated a degree of security implementation and compliance because of its safeguards requirements to protect PHI



Legal Perspective- Liability Issues

- Civil Monetary Penalties- CMPS
- Criminal Exposure
- Civil State Causes of Actions/Theories

Legal Perspective- Civil Liability Issues

- Interim Enforcement Rules
- Published April 17, 2003
- Procedural and substantive requirements for the imposition of Civil Monetary Penalties
- Rule does not address criminal penalties - will be enforced by the Department of Justice

Legal Perspective- Civil Liability Issues

- Will impose penalties on “a person who is a covered entity”
- Person is defined as “a natural or legal person”
- Penalty up to $100 per violation for each such violation (based upon definition of “person” set forth above, appears to be $100 per covered entity per violation)
- Violations of identical requirement or prohibition cannot exceed $25,000 per year

Interim Enforcement Rule

- Defenses to civil monetary penalties as set forth in statute:
  - person did not know and by exercise of reasonable diligence would not have known of the violation
  - violation is due to “reasonable cause” and not “willful neglect” and is corrected within 30 days - or longer at Secretary’s discretion

Interim Enforcement Rule

- CMP may be reduced or waived entirely “to the extent that the payment of such penalty would be excessive relative to the compliance failure involved”

Criminal Enforcement

- Criminal enforcement
  - knowing violations = fine of up to $50,000 and/or imprisonment of up to one year

Criminal Enforcement

- Offenses committed under false pretenses - fines of up to $100,000 and/or five years imprisonment
- Offenses committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm - fines of up to $250,000 and/or ten years in prison

Criminal Enforcement

- First Conviction for HIPAA Rules Violation- August 2004

Criminal Enforcement: Open Issues

- How will “knowingly” be interpreted?
  - Will this be interpreted to mean “knowingly and **willfully**”
  - Note: the False Claims Act does not contain “willfully” and thus many circuits have not required “willful intent” (See U.S. v. Catton, 7th Cir.)

Criminal Enforcement: Open Issues

- Interpretation of “knowingly”
  - Will courts take into account the confusion associated with interpretation of the Privacy Rule (for false claims cases, courts have looked to what guidance is available for providers)?
  - Will courts impute knowledge for reckless disregard/conscious avoidance?
  - Will courts hold physicians to a duty to know and understand HIPAA as they have with billing practices?

Criminal Enforcement: Open Issues

- Who will be subject to criminal penalties?
  - If “person” is defined in same manner as CMP enforcement rule, would only subject “person who is a covered entity” to enforcement?
  - Will criminal liability be imposed on administrators with knowledge of violations as with False Claims Act? Could privacy and security officers with knowledge of violations also be charged?

Criminal Enforcement Risks

- Will covered entity be subject to criminal liability for business associate's actions if covered entity had knowledge of the actions
- "Knowing" violations without ill intent and that do not cause damages could still technically result in criminal penalties - could DOJ use this as leverage for other settlements, etc.

Legal Perspective- Liability Issues

- HIPAA could set standard of care for negligence with respect to state law causes of action
- Potential causes of action:
  - Negligence (malpractice)
  - Implied contract
  - Invasion of Privacy
  - Intentional Infliction of Emotional Distress
  - Slander
  - Fraudulent Misrepresentation

Legal Perspective- Liability Issues

- Saur v Probes, M.D., 190 Mich. App 636 (1991)
  - Patient brought medical malpractice action against psychiatrist for unauthorized disclosure of privileged documentations.
  - Court recognized that licensing statute creates legal duty to protect confidentiality

Legal Perspective- Liability Issues

- West Virginia Hospital- $2.3 million verdict in case where records clerk improperly disclosed patient information for fun (took mental health records to bar, etc.)
- Washington D.C. case -$250,000 jury verdict upheld- part time receptionist at hospital revealed HIV status of a patient to his co-workers (the receptionist worked with the patient at another job)

Legal Perspective- Liability Issues

- What is effect of settling with government in non-confidential agreement if there is a HIPAA violation
  - Can patient/plaintiff use HIPAA violation as evidence of negligence against defendant in breach of privacy action (assuming patient has suffered damages)

Collaboration Case Study

- General approach to the project involving:
  - Legal discipline
  - Consulting/technical discipline

Collaboration Case Study

- Planning and coordinating between attorneys and consultants
- Preparation for on-site meetings/information gathering process
  - Development of mutually acceptable information gathering tools and documents
    - Roles in the development

Risk Analysis- Why, What, How?

Risk Analysis & Management

Under HIPAA each covered entity:

- Assesses its own security risks
- Determines its risk tolerance or risk aversion
- Devises, implements, and maintains appropriate security to address its business requirements
- Documents its security decisions

Risk can either be:

- Mitigated/Reduced (Applying controls)
- Transferred (Insuring against a loss) or
- Accepted (Doing nothing, but recognizing risk)

Risk should be handled in a cost-effective manner relative to the value of the asset

Risk Analysis vs. Gap Analysis

- “If you know the enemy and know yourself, you need not fear the result of a hundred battles. (Risk Analysis)
- If you know yourself and not the enemy, for every victory gained you will also suffer a defeat.” (Gap Analysis)

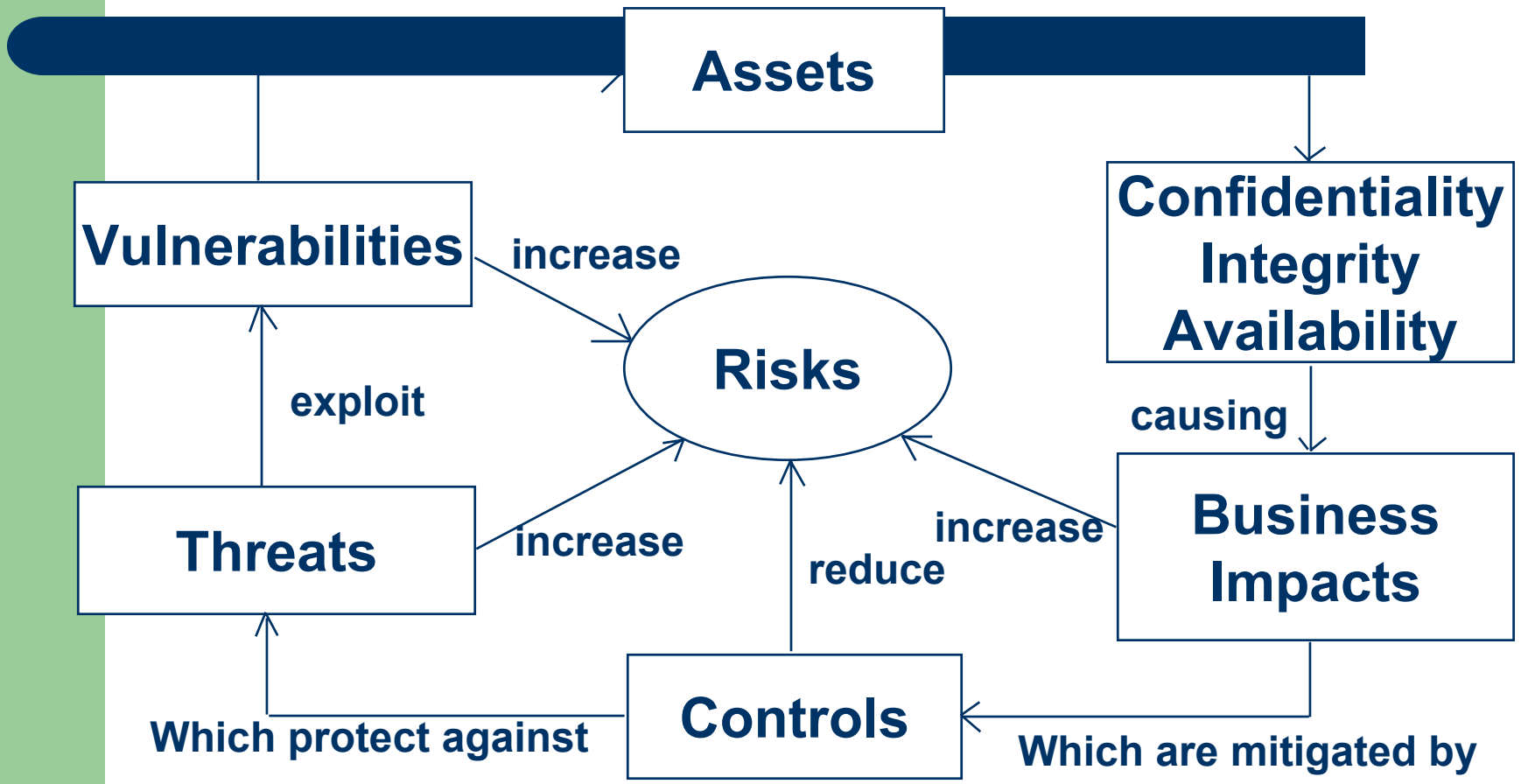
— Sun Tzu (circa 500 B.C.)

- Gap analysis helps identify the vulnerabilities in your information assets;
- Risk analysis examines those vulnerabilities in light of potential threats that can exploit them and their likelihood of occurrence

Risk Analysis

- What needs to be protected?
  (Assets – Hardware, software, data, information, knowledge workers/people)
- What are the possible threats?
  (Acts of nature, Acts of man)
- What are the vulnerabilities that can be exploited by the threats?
- What is the probability or likelihood of a threat exploiting a vulnerability?
- What is the impact to the organization?
- What new controls or safeguards can be implemented to reduce risks to an acceptable level?

Collaboration: Risk Analysis Process



Examples of Typical Vulnerabilities

- Internally
  - PHI on workstations, laptops, biomedical devices, charts, pdas, servers
  - Disposal of PHI
- Externally
  - Vendors with system access
    - Software, biomedical equipment, pda, application service providers/hosting services
  - Business associates
    - Billing and management services
    - Transcription services
    - Data aggregation services

Possible Risks

- Cash flow slowed or stopped
- Fines, penalties, imprisonment, law suits
- Loss or corruption of patient data
- Unauthorized access and/or disclosure
- Loss of physical assets- computers, pdas, facilities
- Patient safety
- Employee safety
- Bad PR

Risk analysis either qualitative (H/M/L) and/or quantitative ($/units/expected values)- need to focus on the "critical few" rather than the "trivial many" ; e.g., securing the network will benefit all of the applications on it!

Collaboration Case Study

- The Risk Analysis Process
  - Documentation
- Attorney/Client privilege issues
  - Drafts and final product

Collaboration Case Study

- Post-information gathering/meetings
  - Roles in the document preparation
- Development of policies
  - Best practices – consultant role
  - Compliance perspective- legal role

Security Best Practices

- Policies, Procedures, Documentation
- Training
- Observation
- Creating user accounts
- Password creation
- Media controls
- Media disposal
- Workstation safeguards

Security Best Practices

- Incident reporting and response
- Audits
- Physical access controls
- E-mail
- Wireless
- Network security
- Personnel clearance, terminations, sanctions

Collaboration Case Study

- Documents for clients and roll-out of security compliance plan
  - Security Program Manual
    - Collaborative input

Questions

- Questions and Answers

Thank You!

- Andrew Wachler
  - awachler@wachler.com
  - 248-544-0888
- John Parmigiani
  - jcparmigiani@comcast.net
  - 410-750-2497