HIPAA: The Realities of Administrative Simplification

Privacy, Security, and Health Information Management

Thomas H. Faris, Esq.
Chief Privacy Officer (CPO)
IMPAC Medical Systems, Inc.

IMPAC

Environment of Controversy

- Failure to follow the intent of HIPAA
- He said, She said, HIPAA says
- Weak interpretations, Strict interpretations
- “I know it’s stupid, but it’s required by HIPAA.”
- Unjustifiable reliance upon the “chosen few”
- Impact on business relationships

IMPAC

HIPAA is Administrative Simplification

- The healthcare industry lobbied for HIPAA to ease the rising cost of healthcare administration
- The Act requires the standardization of the format for electronic data interchange (EDI)
- Pursues the most effective and efficient use of modern information technology
- With the increased ability to aggregate and communicate large amounts of information, Congress felt it necessary to enact regulatory protections for the privacy and security of that information

IMPAC

Side Effect of Information Technology:

- *Constantly advancing technology permits:*
  - the collection and aggregation of large quantities of data,
  - in any desired format or structure,
  - subject to endless permutations of sorting, filtering, and analysis, and
  - the instantaneous widespread distribution of the raw data or analysis results
- *… all without significant human thought.*

IMPAC

Other Reasons to Protect Patient Data

- State Laws, National Law
- Industry Standards
- Right thing to do – Protection of the health care consumers
- Patient legal claims: Negligence

IMPAC

Negligence, regardless of HIPAA

- Failure to perform a duty to use reasonable care.
- Duty of care is a socially defined standard of care for the protection of others against unreasonable risks
- Based upon:
  - Foreseeability of the risk
  - Expectation that the responsible party would prevent the harm
- An industry standard or common practice is evidence of a duty of care

IMPAC

Negligence – T.J. Hooper case

- Tugboat lost barge and cargo during a storm.
- The tugboat had no receiver that would have warned the captain of the storm.
- Very few tugboats had receivers.

Findings:

- The court found the tugboat owner negligent:
- Whether industry practice or not, the service provider has a duty to use new and available devices to protect the customer from unreasonable risk.

IMPAC

Privacy vs. Security

- A team of protections to prevent unintended access, use, or disclosure of confidential information
- Significant overlap between concepts and regs
- “Privacy” – The requirements of restricting access, use, or disclosure (the ends)
- “Security” – Operational, physical, and technical protections to support privacy restrictions (the means)
- However (a chicken-egg loop):
  - Privacy requires adequate security
  - Security – A major objective is confidentiality (privacy)

IMPAC

Privacy vs. Security: Result

- Organizational Privacy and Security protections are interwoven into a single system of operational and technical protections.
- Difficult to implement one without the other.
- Privacy/Security Management will need to determine what levels of security are necessary at this time.

IMPAC

Privacy

- Prevents the unreasonable offense of a patient's interest in restricting unnecessary knowledge of personal information provided or accumulated to assist in their diagnosis or treatment; however
  - Data is necessary for diagnosis and treatment
  - Organizations require business records
  - Complete protection is impracticable
  - Healthcare requires significant disclosure
  - Society has interests in the disclosure of certain information

IMPAC

HIPAA Privacy: Basic components (overview only!)

- Notification of privacy practices
- Individual right of control
  - Can deny use, request restrictions
  - Authorizations
- Organizational control of PHI
  - Minimum necessary
  - Limited privileged use (TPO) and disclosure (Itemized privileges)
  - Disclosure accounting
  - Incidental disclosures are acceptable

IMPAC

HIPAA Privacy: Basic components (overview only!)

- Current & accurate information
- Culture of confidentiality
  - Policies and procedures
  - Training
  - Business Associate controls\
  - Complaint handling
- Use of de-identified information

IMPAC

Security

- A comprehensive system of operational, physical, and technical protections implemented to prevent unintended access, use, and disclosure of PHI.
- *Confidentiality* – Protection of entrusted information from unauthorized use, access, or disclosure.
- *Integrity* – Preservation of the specific nature, character, and content of the information.
- *Availability* – Ability to access, use, or disclose information as intended in an effective and efficient time, place, and manner.

IMPAC

Security, However:

Don't Go Overboard!

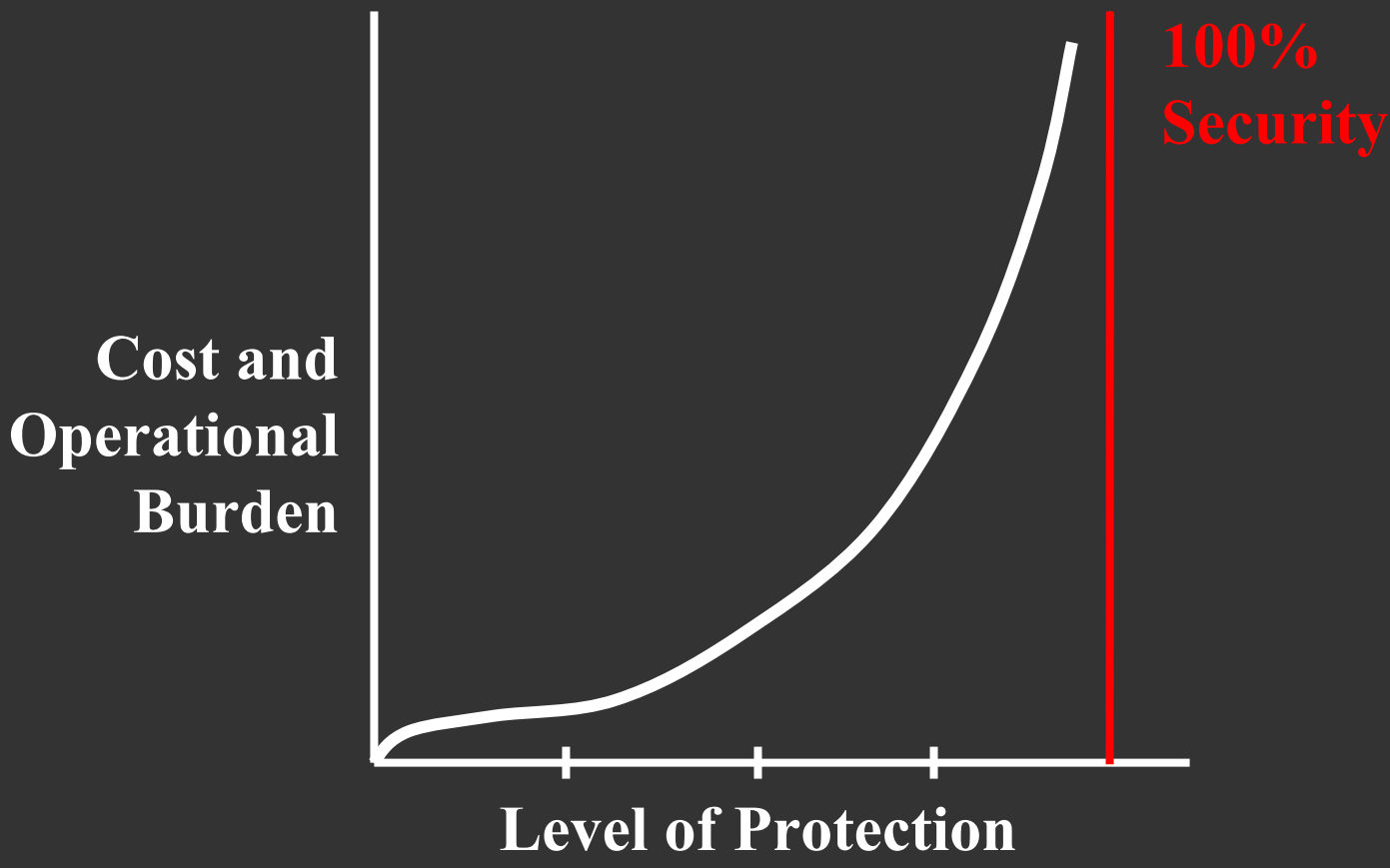
- Data can be ultimately protected if it is never captured
- All further use or disclosure can be halted

But,

- Data is captured because we find value in it's use and we must be free to use it accordingly with reasonable protection
- The newest technology may be effective, but very expensive and unwieldy

IMPAC

Cost-Risk Analysis



Security: HIPAA Intent

- Technology neutral
- Scalable
- Cost-Risk analysis
- Organization determined requirements
- “Reasonable” standard

IMPAC

Security: Operational Policies and Procedures

- Security Management Planning
- Security Configuration Management
- Management Responsibility
- Information Handling Procedures
- Access Controls (Operational)
- Information Technology Use Policies
- Employee Training
- Disciplinary Action
- Employee Termination

IMPAC

Security: Operational Policies and Procedures

- Vendor / Associate Controls
- Internal Auditing
- Contingency / Disaster Recovery Planning
- Incident Handling
- Compliance Certification

IMPAC

Security: Physical Safeguards

Physical safeguards to prevent unreasonable threats to an organization's buildings, equipment, media, and accessible data.

- Locks
- Physical barriers
- Monitoring
- Visitor control
- Control of media
- Control of equipment
- Corporate security culturing

IMPAC

Security: Technical Security Mechanisms

Security technology must be implemented to protect information stored on a computer network or otherwise electronically communicated from unauthorized access, use, or disclosure.

- Virus Protection
- Perimeter Defense, Intrusion Detection
- Secure Communication
- Access Controls, Authentication
- Audit Trail, Alarms

IMPAC

Points to take Home!

- Don’t fall for the current HIPAA hype
- All entities should be concerned with privacy and security of confidential information
- Privacy and security comprise an interwoven system of data protection
- Be “reasonable” when implementing privacy and security protection

IMPAC

Thank you!

For more information or questions:

IMPAC website:

www.impac.com (click on HIPAA link)

Email:

Tfaris@impac.com

IMPAC