Privacy Enhancing Technologies

June 9, 2002

Thomas H. Faris, Esq.

Problem:

- *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.*

Problem:

- *How do we determine and implement adequate and appropriate technical protection for the personal patient information?*

Why Worry About Patient Data Privacy?

- *New Regulations:*
  - *Health Insurance Portability and Accountability Act (HIPAA)*
  - *Personal information and Protection of Electronic Documents Act (PIPED)*
  - *EU Regulations: BS/ISO/IEC 17799*
- *State Law*
- *Right thing to do – Protection of the health care consumers*
- *Negligence – A reasonable duty to protect patient Data*

Negligence – T.J. Hooper case

- *Setting the rule (1928):*
- *Tug boat lost barge and coal during a storm. Barge owner claimed negligence because the Tug didn't have a weather radio.*
- *Supreme Court found that there is a duty to keep up with technological innovations that set the standard of care in the industry. A breach of that duty of care is actionable negligence.*

Don't go overboard

- *Data can be ultimately protected if it is never captured*
- *Data can be locked from any further use*

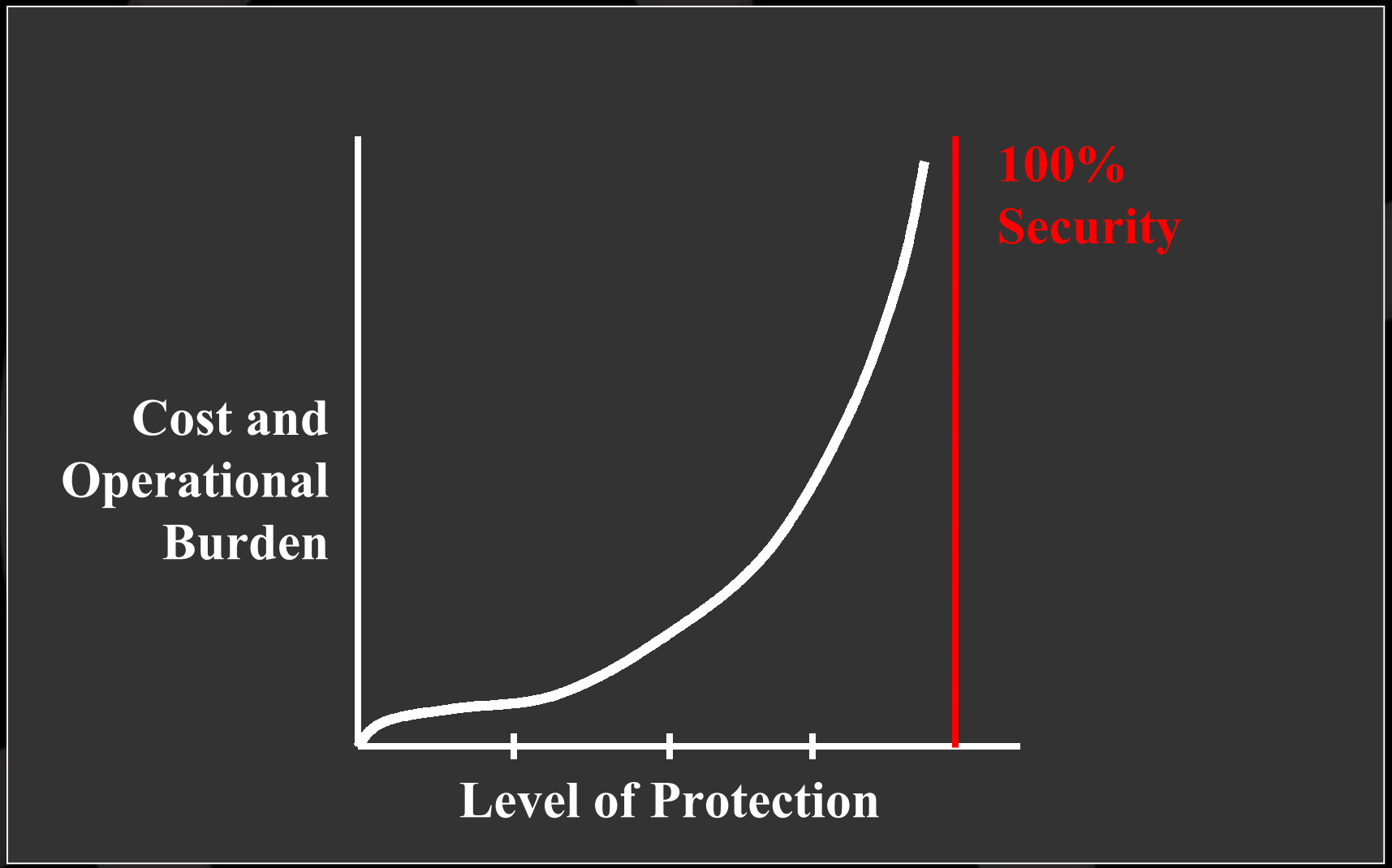
However:

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

Cost-Risk Analysis

- *A due diligence analysis must be performed to determine what is reasonable and appropriate*
- *Risk Mapping / Data Flow Analysis*
- *Balance the cost of the safeguard against the gravity of the privacy risk*
- *The safeguard should not unreasonably burden treatment, billing, or other health care operations*

Cost-Risk Analysis



Privacy vs. Security

What is "Privacy"

1. *The right to be left alone*
2. *Operational controls over the access, use, and disclosure of data by those with such privilege.*

Privacy vs. Security

What is "Security"

1. *The technical or physical means of assuring privacy*
2. *Operational controls over or technical protections of data from unknown or unprivileged third parties.*

Privacy vs. Security

What is "Security"

C – Confidentiality

Access only by authorized parties

I – Integrity

Authentic and reliable data

A – Availability

Data is accessible when and where it's supposed to be

Privacy vs. Security

"Privacy" and "Security" are inextricably interwoven into a comprehensive system of protecting confidential information

Frontline Privacy and Security Protection (Briefly)

- *Operational Management System*
  - *Security Policies*
  - *Privacy Policies*
  - *Operational Procedures*
- *Appointed responsible party to oversee operations*
- *Clarify relationships and responsibilities with business associates*

Basic Security Protections for Data Privacy

- *Firewalls*
  - *Basic perimeter*
  - *First layer protection*
  - *Reasonably inexpensive*
  - *Necessary for any open system potential contact*

Basic Security Protections for Data Privacy

- *Intrusion Detection*
  - *Means to determine whether there have been likely attempts to enter the system without proper authentication*
  - *Typically maintains an audit trail and alarms*
  - *Can also be used to monitor internal activity*

Basic Security Protections for Data Privacy

- *User Authentication*
  - *Passwords*
  - *Biometric*
  - *Tokens*

Basic Security Protections for Data Privacy

- *Communication Protection*
  - *Dedicated lines*
  - *Virtual Private Networks (VPN's)*
  - *Encryption*
    - *No prescribed requirement*
    - *Industry standard should be minimal*
    - *3x DES – appears to be developing standard*

Basic Security Protections for Data Privacy

- *Virus Protection*
  - *Protection from viruses, worms, malicious code, etc.*
  - *Now, with content screening*

Privacy Enhancements

- *Access Controls*
  - *Role, User, or Group access privileges*
  - *Provide or limit access to specified information*
  - *Configurable to meet organizational requirements*
- *However:*
  - *Must provide access to needed information*
  - *Must provide some administrative override*

Privacy Enhancements

- *Elevated Authentication*
  - *Permits additional scrutiny of user verification and privilege*
  - *Initial user can remain logged into the application while performing a more secure role specific task*
  - *overrides, extremely confidential data, important warnings, sign-offs …*

Privacy Enhancements

- *Audit Trails*
  - *Uneditable recording of significant access, use, and disclosure*
  - *Identifies accountable party and privilege utilized*
  - *Currently debated in industry:*
    - *Consensus indicates interest in tracking significant decisions, disclosures, and significant access.*
    - *Tracking every view access of information is impracticable.*

Privacy Enhancements

- *Alarms/Alerts/Monitoring*
  - *Contingency monitoring and reporting*
  - *Alarms can be provided if recognized or suspicious activity is detected*

Privacy Enhancements

- *Auto Logoff*
  - *Users automatically logged off due to application inactivity*
  - *Prevents exploitation of logged user's access privileges*
  - *Configurable, to meet organizational requirements*

Privacy Enhancements

- *Email filtering and screening*
  - *Email is inherently insecure and widely utilized for the transfer of confidential information*
  - *Crosses an open system, so needs to be encrypted for protection*
  - *Screening can discover unprotected confidential information for redaction or message capture*

Electronic Medical Records / Registry Applications

- *Privilege restriction*
- *Authentication*
- *Duplication restriction*
- *Access and activity monitoring / Audit Trail*
- *Alarms / Auto-Logoff*
- *Automation for efficiency and accuracy*
- *Remove many human error elements*
- *Immediately available information*
- *Consistent communication with associates*

New technology – ASP's, PDA's, Wireless devices

- *Increased availability of information*
- *Very beneficial to operations*
- *Confidentiality and Integrity concerns - as long as privacy/security technology keeps up and is used*
- *Technology is out there, must make sure that it is used correctly*
- *Ensure vendors have considered and mitigated any privacy and security concerns*

Thank you!

Thomas H. Faris, Esq.
IMPAC Medical Systems, Inc.
Chief Privacy Officer
Tfaris@impac.com