What Does HIPAA Really Say About Web-Based Information?

June 9, 2002

Thomas H. Faris, Esq.

IMPAC

Problem Statement:

- The Internet:
  - One of the world's most active forms of communication
  - Very high data security risk
  - Traditionally used in a non-protected manner
  - Permits the exploitation of countless numbers of systems by i… hackers

"Why? Because We Can"
Slogan from DEF CON III

- Is a cost-efficient significant technology solution for the transfer, accumulation, and availability

Problem Statement:

- How do we safely harness the value and ease of this inherently insecure means of modern communication, especially in light of HIPAA and related privacy and security regulations?

Problem: Consumer Confidence

HIPAA Preamble:

"…75 percent of consumers seeking health information on the internet are concerned or very concerned about the health sites they visit sharing their personal health information with a third party without their permission."

Ethics Survey of Consumer Attitudes about Health Web Sites, California Health Care Foundation (Jan 2000)

HIPAA - Health Insurance Portability and Accountability Act

Administrative Simplification:

- Privacy
- Security
- Transactions and Code Sets

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

HIPAA: Privacy

- Covered entities must take reasonable steps to ensure that protected patient information is not used by or disclosed to any parties that do have a valid need to access the data
- Only those involved in treatment, billing, or health care operations may use or receive disclosures of the protected health information
- All use and access must be the minimum necessary to accomplished the privileged use
- The patient must provide specific authorization for any other use or disclosure

HIPAA: Security

Procedures and technology must be in place to protect the

- Confidentiality
- Integrity
- Availability

of ALL information related to the healthcare or payment for provision of healthcare of an individual.

HIPAA: Security

- General operational procedures
- Physical safeguards
- Technical information system level functional procedures
- Technical Security Mechanisms

Internet Use in the Healthcare Industry

- Provide Information to patients / Informational websites
- Web-based applications
- Application Service Providers (ASP)
- Communication of data / Data Submissions
- Connecting organizational facilities
- Aggregation / Evaluation of research or other data
- Email distribution
- Lab reporting

What does HIPAA explicitly say about the Internet?

Only:

Encryption should be used whenever protected health information maintained or transmitted in an open system.

However, the inherent risk in the use of the internet must be considered when implementing other HIPAA requirements for your organization.

HIPAA Compliance Objectives

Security NPRM, Section 142.308

All applicable entities must assess risks and vulnerability to individual health data in its possession and develop, implement, and maintain appropriate documented security measures.

HIPAA and the Use of the Internet

- Administrative Simplification promotes the most efficient use of technology to meet operational needs of the health care industry
- Common sense privacy and security mechanisms must be put into place to protect patient health information
- Specific implementations are dependent upon each Covered Entity's assessment of their specific vulnerabilities
- The Internet is an open system with the potential for accessibility by many unknown parties
- The Internet's higher level threats to security

Vulnerability Analysis

- Know your threats
  - Data Flow Model
- Evaluate the criticality of your vulnerabilities
  - Likelihood of occurrence
  - Severity of outcome
- Establish necessary mitigations
  - Technical
  - Procedural

Significant Internet Security Risks

- Interception of clear text packets
- Hacking – any connection to the web is vulnerable
- Authentication breach
  - Password cracking
  - Password interception or theft
  - Spoofing
- Viruses, worms, trojans
- Wireless Interception
- Equipment Failure
  - Security Breach
  - Downtime

Reasonable Protections

- Administrative Simplification – the most efficient administration and operation of the organization using modern technology
- Common-sense protection of the privacy and security of the data is what is required
- HIPAA does not require an absolute bar on use and access
- HIPAA is technology neutral and scalable

Reasonable Protections

- HIPAA was never intended to thwart treatment, payment, or other related health care operations, including association and interactions with third parties
- Mandated or voluntary industry standards often provide a basis for what is "reasonable" and should be evaluated
- Must balance the risk against cost and efficiency considerations

General HIPAA & Internet Considerations

- A simplified introduction to some of the most important issues to address
- Excluding technical considerations:
  - Specific Internet Protocol use
  - Cryptography key selection and management
  - Site design technologies
- Disclaimer: This is a very simplified view of these concepts, just to point you in the right direction

General Protection of Patient Health Information

- Patient Health Information must be protected regardless of where it is maintained:
  - Onsite
  - Website
  - Third party vendor or business Associate
- The Covered Entity must ensure that the protected data is accessed, used, and disclosed in accordance with HIPAA at all times

Minimum Necessary Rule Still Applies

- All use, access, and disclosure must be the minimum necessary to accomplished the privileged use
- Information may be access or used by or disclosed to any associated third party for the purpose of treatment, billing, or health care operations
- Includes data aggregation, coding or other processing, organization support (such as information services or ASP)
- Other uses may require patient authorization

Aggregation Results may be Displayed if De-identified

- If the web activity provides a data aggregation function, the data must be de-identified
- Aggregation for quality assurance of health care operations is a privileged use of protected health information

Business Associates

- Associates performing functions for the Covered Entity must be covered by a Business Associate Agreement to comply with the rules in the HIPAA regulations
- Covered Entity must reasonably assure itself that associate can meet requirements:
  - Adequate security: Protected equipment, technical security, adequate concern over data handling, operational procedures.
  - Adequate privacy: Understands HIPAA and related requirements, responsible person(s), access controlled. Control of its associates.

Web Activity Must be Subject to Administrative Protections – Privacy and Security

- Responsible party to ensure compliance with requirements
- Training provided to all that may use, access, control, of disclose any protected health information
- Complaint process for reporting possible violations of policies
- Document all policies and procedures to ensure adequate privacy and security of the web activity
- Means for the individual to amend or correct the data
- Audit for effectiveness of technical and

Physical Security

- Web related equipment is often stored away from typical data handling mechanism – easily forgotten
- Access to servers, workstations, and other equipment must be restricted to prevent improper access, use, or disclosure
- Redundancy
- Validation of Effectiveness
- Assurances that Business Associate can secure equipment

Encryption

- Encryption is required for “Open” systems
- Communication across open systems
  - Internet
  - Collaborative networks
  - Email
- Data sitting on an open system
  - Bare databases with no authentication/access controls
  - Sitting clear text data or files

Encryption (Con't)

- No specific technology or level of protection is required
- Depends on cost-benefit vulnerability analysis
- Should keep up with industry standards

Email

- Fast, easy, cheap, effective
- Dominant communication form of the modern workplace
- Typically, Simple Mail Transfer Protocol (SMTP) – stored and forwarded from multiple rely points, all of which may capture unprotected data
- Must use adequate encryption to protect
- Should scan unprotected email for protected information to either:
  - Remove the information
  - Prevent the distribution of the suspicious

Firewalls

- Primary perimeter protection – the first line of defense
- Provides and control communication access points into and out of your computer system
- Security degrades with every opening
- No specific technology required, see you vulnerability analysis
- Should be utilized any time a hard line is not used
- “Only as good as you let it stay”

Intrusion Detection

- Just about every system connected to the outside world is "hit" at some point
- Most never know it
- Intrusion detection must be implemented to recognize suspicious contacts and intentional attacks
- Helps to identify probes and scans attempting to find perimeter vulnerabilities
- 24 hour monitoring process – watch out when school is out

Virus Protection

- Don't trust data or files from the web, no matter the source
- Someone else's vulnerability could become yours
- Always use adequate virus protection
- Keep up to date
- This is common sense

Qualified Security Professional(s) for Web Operations

- System design and maintenance
- Continuous monitoring
- Proactive awareness
  - Evolving industry standards
  - Application patches
  - Security alerts and recommendations
- Trained and prepared to handle breaches and failures
- Recognize and resolve vulnerabilities
- Consultants may be useful, but on a routine basis

Authentication

- Must verify that user is actually the user before permitting access
- Actual individual verification, not just a simple identification (such as a SSN for a patient)
- Password protections, biometrics, tokens
- Handshake may be used for a trust relationship

Authentication – Password Protections

- Typical suggestions
  - Min Length
  - Mixed characters
- Routine expiration
- Logins shall lock after repeated failures, except for physically secure internal administrative stations
- Careful of requirements for patient access

Access Control

- User must have privilege and need to access particular data
  - Privileged employees
  - Administrative Personnel
  - Business Partners
  - Patients (their own)
- Minimum Necessary
- Must prevent unreasonable possibility of unnecessary, inadvertent, or wrongful access to protected information
- Maintain records of all authorized access
- Access Termination

Auto Logoff

- Termination of unused connections
- Prevent unauthorized access, especially when user not present

Incident Handling

- Problem reporting mechanisms
- Alerts / Alarms
- Process in place to mitigate effect of an unauthorized release of data or failure of a security mechanism
- Reporting relationship with law enforcement agency

Contingency Planning / Disaster Recovery

- Data Archives
- Redundant Systems to ensure “up time”
- Plan to quickly respond to all significant failures and restore operations with little or no loss of information
- Plan for alternate operation in case of disaster
  - Site destruction
  - Earthquake, flood, fire, power outage, meteor
- What must be done to maintain the intended use of the web activity if …?

Wireless Technology / PDA's

- Becoming very popular
- Very insecure
  - Message interception
  - Loss and access
- Strong password/authentication
- Encryption
- Procedural controls for storage of protected health information

Additional Regulations

- Regulations in the works, many already enacted
- International regulation
- A growing trend of protecting personal information
- Developing a Standard of Care

Thank you!

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

IMPAC