MEDePASS

Health Care Data Security: HIPAA Draft Security Rules and California Law

California Health Care Symposium 2001

May 10, 2001

Steven M. Fleisher,
VP & General Counsel
MEDePASS, Inc.

MEDePASS

Introduction

- Overview of Issues at Basic Level
- Assume you Work for a Covered Entity or one who does Business with a CE
- Mostly about HIPAA Security Reg
- Focus: appreciation, assessment and preparation getting prepared

MEDePASS

Topics of Discussion

- Status
- Overview
- Four Security Standards Areas + Electronic Signatures
- Preemption
- California Laws
- Implementation Issues
- Conclusions
- References

MEDePASS

Status of the Security Regulation

- Proposed rule issued August 12, 1998
  - (63 FR 43241)
- Final Not Published by the Clinton Administration
- Latest Gossip & Unverified Rumors From DHHS
- Why Take Seriously Now?

MEDePASS

Who is Regulated? ("Covered Entities" in HIPAAspeak)

- Providers of Healthcare
- Healthcare Clearinghouses
- Health Plans
- Which electronically maintain, process or transfer PIHI (aka IIHI)

MEDePASS

Those Indirectly Regulated

- Those with whom Covered Entities Exchange PIHI (Must enter into “Chain of Trust” Agreements)

MEDePASS

Security vs Privacy

- The two standards are inextricably entwined:
  - Security Standard requires *administrative, technical and physical measures* to guard the data integrity, availability and confidentiality (§164.530)
  - Privacy Regulation that appropriate *administrative, technical and physical safeguards* be in place to protect protect privacy of health info (§ 142.308)

MEDePASS

Security vs Privacy

- Security: the physical & electronic protection of private information
- Privacy: limiting access to that information to those authorized

MEDePASS

Statutory Standard for HIPAA Security

- Each person…who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards—

MEDePASS

Statutory Standard(II)

- (A) to ensure the integrity and confidentiality of the information; and
- (B) to protect against reasonably anticipated
  - (i) threats or hazards to the security or integrity of the information
  - (ii) unauthorized uses or disclosures of the information; and
- (C) Otherwise to ensure compliance with this part by the officers and employees of such person

(42 USC § 1320d-2(d))

MEDePASS

Penalties

- Favorite scare tactic but take seriously
- Civil: $100/violation; $25,000 annual limit
- Criminal: knowing wrongful disclosure of PIHI:
  - One year and $50,000
  - False Pretenses: 5 years and $100,000
  - Intent to use for personal advantage or gain, malicious harm: 10 years and $250,000
- Focus on intent to profit from unlawful disclosure

MEDePASS

Four HIPAA Security Standards

- Administrative Procedures
- Physical Safeguards
- Technical Security Service
- Technical Security Mechanisms
- [Electronic Signatures (separate rule)]

MEDePASS

Administrative Procedures

- 12 requirements
- Each must be documented, reviewed and updated periodically
- Each comes with a list of implementation requirements

MEDePASS

Administrative Procedures (II)

- Certification
- Chain of trust agreement
- Contingency plan
- Records processing
- Information access control
- Internal audit
- Personnel security

MEDePASS

Administrative Procedures (III)

- Security configuration management
- Security incident procedures
- Security management process
- Termination procedures
- Training

MEDePASS

Physical Safeguards

- Assigned security responsibility
- Media controls
- Physical access controls
- Workstation policy
- Secure workstation location
- Security awareness training

MEDePASS

Technical Security Services

- Access control
- Audit controls
- Authorization control
- Data authentication
- Entity authentication

MEDePASS

Technical Security Mechanisms

- Integrity Controls
- Message Authentication; and
- Encryption or access controls
- Also alarms, audit trails, entity authentication and event reporting

MEDePASS

Electronic Signatures

- Electronic signatures not currently required; if used, this standard applies requiring a digital signature
- Implementation features:
  - Message integrity
  - Nonrepudiation
  - User authentication

MEDePASS

Relationship of HIPAA to State Law: Preemption Issues

- HIPAA "preempts" any "contrary" provision of state law
- Includes state legal requirements that health records be in writing rather than electronic form
- Three types of limitations on the general rule

MEDePASS

Preemption (II)

- Exceptions
  - A. Public Health Laws (injury , child abuse, birth, death and disease reporting, public health surveillance, investigation or intervention)
  - B. State Regulatory Reporting (requiring health plans to report or provide access to info for management or financial audits, progress monitoring & evaluation, facility or individual licensure or certification)

MEDePASS

Preemption (III)

- C. Determination by the Secretary
  - If the Secretary determines a state rule is necessary to
    - To prevent fraud & abuse;
    - To regulate health plans and insurance;
    - Health care delivery or cost reporting; or
    - For other purposes; or
  - Addresses controlled substances; or
  - Relates to privacy of IIHI and is more stringent than federal law (42 USC § 1320d-7)

MEDePASS

Preemption procedures

- There will be a process (as under the privacy reg) to request the Secretary to determine whether a state rule is preempted.
- Written request by state agency
- Regs control until a determination made

MEDePASS

California Health Information Security Law

- Excellent *confidentiality and privacy* rules regarding IIHI
- Very little explicitly on SECURITY
- Why? No one paid attention until now (now = HIPAA)
- Healthcare: a cottage industry where caring is sharing

MEDePASS

California Health Information Security Laws

- Numerous state laws protecting *disclosure*, including negligent disclosure or destruction *(e.g., Civ Code §56.30)*
- No mention of security but if lax security, risk negligent disclosure and liability

MEDePASS

California Health Information Security Laws (II)

- Licensed health facility record keeping law (Health & Safety Code §123149)
  - Applies only to such licensed facilities that keep no paper records
  - Requires offsite storage, document integrity mechanism
  - Prevent unauthorized access
  - Record authentication

MEDePASS

California Health Information Security Laws (III)

- Telemedicine law (Bus & Prof §2290.5)
  - Prevent unauthorized access to patient identifiable images in transmission
- Prescription Records (Health & Safety §11164.5)
  - Electronic records of Rxs must be securely maintained and able to track changes

MEDePASS

Ethical Guidelines

- AMA Ethics Opinion 5.07 re computerized medical record confidentiality:
  - Control access with passwords, encryption, hardware tokens, etc.
  - Identify persons with access
  - Audit trail re use of and changes to information

MEDePASS

JCAHO

- Information Management Planning IM-2 (confidentiality, security & integrity of data maintained)
  - Access control through passwords codes and audit trails
  - Protection against unauthorized intrusion, corruption or damage
  - Correction procedures

MEDePASS

HIPAA Implementation

- HIPAA compliance is achieved at an *institutional* level (large or small)
- To implement this high level of security, a change in culture is required. *That is the big deal*
- Neither software, hardware nor HIPAA consultants are "HIPAA compliant"

MEDePASS

HIPAA Implementation (II)

- No specific technology is required
- Intended to be scalable to the size of the enterprise
- Start planning and budgeting Now
- *Do a GAP analysis ASAP (everyone)*
- *Biggest risk is internal*
- This is not just an IT project

MEDePASS

Implementation (III)

- Need to get together a team if possible
- Check with vendors re HIPAA "compliance" on legacy soft/hardware
- Get HIPAA warranty for new stuff
- Keep a legal risk mindset since these regs will raise the duty of care standard
- Small medical groups look to CMA and other organizations for assistance

MEDePASS

Conclusions

- There is a significant business case for HIPAA implementation:
  - **significant cost savings and risk reduction**
  - **genuine improvement in PIHI protection**
- HIPAA can induce providers and patients to really trust the internet
- Balance cost and risk reduction
- Perfection is not required; due diligence is
- This will be an ongoing process not a one-time exercise

MEDePASS

Conclusions (II)

- Start NOW (if you haven't already) because you are trying to effect a *change in culture*

MEDePASS

References

- www.aspe.hhs.gov/adminsimp
- www.hipaalawyer.com
- www.tunitas.com
- www.wedi.com
- www.afehct.com
- www.astm.org
- www.cpri.org

MEDePASS, Inc.

- Steven M. Fleisher, V.P. & General Counsel
- MEDePas, Inc.
- 221 Main Street, 3rd Floor
- San Francisco, Ca 94105
- T: 415.882.5159
- F: 415.882.5143
- e: *sfleisher@medepass.com*