Implementing HIPPA Security – An Introductory Briefing

Richard D. Marks

Davis Wright Tremaine LLP

(202) 508-6611

richardmarks@dwt.com

Today's First Premise

It's time to initiate HIPAA projects because

- Time is Short
- The security and privacy requirements are a whole new ballgame
- The technology is not mature and probably is expensive
- The cultural change from new business processes may be wrenching

Question: how to begin? What to do?

Today's Second Premise

Your top management doesn't want to spend money on still-proposed regulations or on unproven technology

Most senior managers are unsure about how to approach HIPAA generally, and specifically regarding:

New business processes & cultural change
New technology
Applicable legal standards

HIPAA – Statutory Standard

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

- (A) to ensure the integrity and confidentiality of the information; and
- (B) to protect against any reasonably anticipated
- (i) threats or hazards to the security or integrity of the information; and
- (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."

The Ratcheting Legal Standard

The T.J. Hooper case

- Large Island Sound – storm comes up, tug loses barge
- Plaintiff barge owner: captain was negligent because he had no weather ratio
- Learned Hand, J.: You are correct, sir!
  - Rationale: to avoid negligence, keep up with technological innovations – they set the standard of care in the industry

Medical Malpractice as a frame of reference

What is the industry standard of care?

- The HIPAA security rules were abstracted from now being imposed on health care.
- So the industry frame of reference is the military-industrial complex.
  - NSA sets the rules
    - At its best, the security is awesome
    - Then there's John Deutsch and Wen Ho Lee (and many others)

HIPAA Applies To

Health Information

Stored or transmitted electronically

By “Covered Entities”

- Health care providers
- Health plans
- Health clearinghouse

Others

- Employers, plans, insurers, marketers, others that use electronic health records

The FEAR

Once patient's records are stored electronically on networks, a couple of clicks can transmit those records instantly all over the world!

Civil Penalties for Violating HIPAA Standards

$100 for each violation

$25,000 annual limit “for all violations of an identical prohibition or requirement”

Criminal Penalties for Knowing Wrongful Disclosure of PHI

1 year and $50,000

False pretenses: 5 years & $100,000

Advantage, personal gain, malicious harm: 10 years & 250,000

HIPAA Security Standards

The Security Standards must

- be comprehensive
- address all aspects of security in a concerted fashion
- be technology-neutral (technology changes quickly)
- be scaleable

Standards – A Matrix

- ✓ Administrative Procedures
- ✓ Physical Safeguards
- ✓ Technical Security Services (data storage)
- ✓ Technical Security Mechanisms (data transmission)

Administrative Procedures

- ✓ Certification ("as part of, and in support of, the accreditation process")
- ✓ Chain of trust partner agreement (akin to business partner agreement under proposed privacy rules)
- ✓ Contingency plan
- ✓ Formal mechanism for processing records
- ✓ Information access control
- ✓ Internal audit

Physical Safeguards

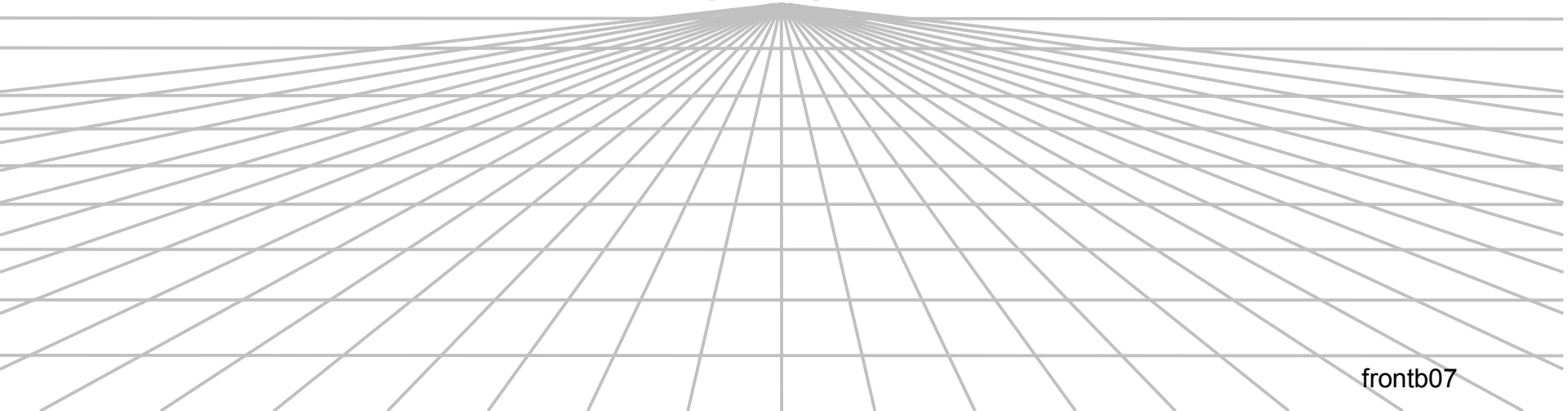
- ✓ Assigned Security Responsibility
- ✓ Media Controls (formal, documented policies)
- ✓ Physical Access Controls
- ✓ Policy on Workstation Use
- ✓ Secure Workstation Location
- ✓ Security Awareness Training

Technical Security Services (Data at Rest)

- ✓ Access Control
  - Documented procedures for emergency access
  - Text-, role-, or user-based access
  - Encryption optional
- ✓ Audit Controls
- ✓ Data Authentication
- ✓ Entity Authentication
  - Auto logoff
  - Unique user identifier for tracking
  - Biometric, password, or other personal identifier

Administrative Procedures

Certification. Each affected organization would be required to evaluate its computer system(s) or network design(s) to certify that the appropriate security has been implemented. This evaluation could be performed internally or by an external accrediting agency.



Technical Security Mechanisms (Data in Transit)

- ✓ For each organization that uses communications or networks
- ✓ Protect communications containing health information that are transmitted electronically over open networks, so that they cannot be easily intercepted and interpreted
- ✓ Over open networks, some form of encryption required

  Integrity control

  Message authentication
- ✓ Network controls

  abnormal condition alarm

  audit trail to facilitate a security audit

  irrefutable entity authentication

  event reporting for operational irregularities

HIPAA Compliance Requires Encryption

- ✓ No other practical way to meet the privacy and security requirements
- ✓ HHS is fully aware the encryption will be necessary
- ✓ HHS may not be aware that

  "Covered entities" typically interconnect (cobble together?) disparate systems from a variety of vendors

  "Covered entities" can't buy an end-to-end solution process changes) won't be easy and will be expensive

Security: Can You Trust the Message?

Is the message sent by the apparent sender?

- Authenticity

Has the message been tampered with (altered)?

- Integrity

Has the message been ready someone who should not see it?

- Secrecy

Why is Trust Important?

Nonrepudiation

Money – and medical records – will move or be changed!

Must be able to prove

[1] Contract or authorization exits

[2] Its terms or other content

Public Key Infrastructure (PKI) Technology

Performs all these functions automatically

Must be engineered for the industry ("technically mature")

E.g., financial industry

At the moment, it's not engineered for health care

Ask the system vendors – be alert for vaporware

Tomorrow's session

Certification Authorities in a PKI System

- Must control the ISSUANCE and STATUS of digital certificates

  People leave

  People are found to be untrustworthy

- Significant expense in CA's administering digital certificates

  There are liability issues, e.g., what if the CA is spoofed into a false certification?

  How allocate the risk? Contracts; insurance

Electronic Transactions – ESign

- ✓ Is an electronic message legally binding?

  Traditional formalities: paper & signature

- ✓ Can you trust the message?
- ✓ What are the rules of conduct?

  When is an electronic message deemed "received"?

  When is an electronic message enforceable?

Legal Tasks in PKI System

- ✓ Certification Practice Statement

  Explains CA's digital certificate issuance and revocation policies
- ✓ Certificate Policy

  Specifies conditions of use of a digital certificate
- ✓ Contracts allocating liability among entity, CA, users

  Insurance and limitation of liability issues

  Federal law: Esign

  State contract law (UCC, UCITA, UETA, etc.)

Certification Authorities

www.verisign.com

www.cybertrust.com

www.cylink.com

www.xcert.com

Systems, akin to VPNs

Big Problems with PKI

- ✓ Expensive to administer: $30 per twice that)
- ✓ Slows down most existing systems
- ✓ Some legacy systems can't be adapted to PKI
- ✓ No standard = no interoperability

  (this is a ***huge, very real, impediment***)

Alternatives to PKI

- VPNs
  - Not as secure as PKI, unless they incorporate PKI practice in the industry?
  - Suffice for the moment as an acceptable practice in the industry?
- Not much else. . . .

  "Currently there are not technically mature techniques…[for] nonrepudiation in an open network environment, in the absence of trusted techniques."

Adding PKI Encryption to Medical System

- ✓ No end-to-end solution on the market
- ✓ "Kluged" systems are tough enough to operate without encryption
- ✓ Some legacy systems cannot be adapted to encryption
- ✓ PKI engineering challenge: volume & speed

  Experience: adding PKI = molasses
- ✓ Unknown Territory! (This is not trivial!)

Industry Overview

- ✓Vendors are beginning to enter the field
- ✓Health IS vendors are working on approaches to integration with encryption packages
- ✓BUT – a lot of vaporware!

Caveats

- ✓ Encryption itself can't do the job alone
  Systems approach to implementation
- ✓ Experience teaches that computer technology projects are difficult to implement well
- ✓ Most organizations are not used to living with HIPAA's level of security (e.g., constant access control, entity authentication, and surveillance)
- ✓ There's a significant litigation potential and substantial jeopardy to individuals

Access is a Separate Set of Issues

- How do you control who is really using the key to which the certificate relates?
  Password
  Password (PIN)plus
    Secure ID?
    Smart Card?
- How do you pay to administer all this?
  Industry experience: costs rise steeply well before 1,000 cards, tokens, or whatever

HIPAA Emergency Access

- ✓ "Glass-break"
- ✓ What's the
  - Procedure?
  - Civil and criminal liability?
    - HIPAA
    - Tort (state law – med mal)

Initial Steps in Implementing HIPAA Security

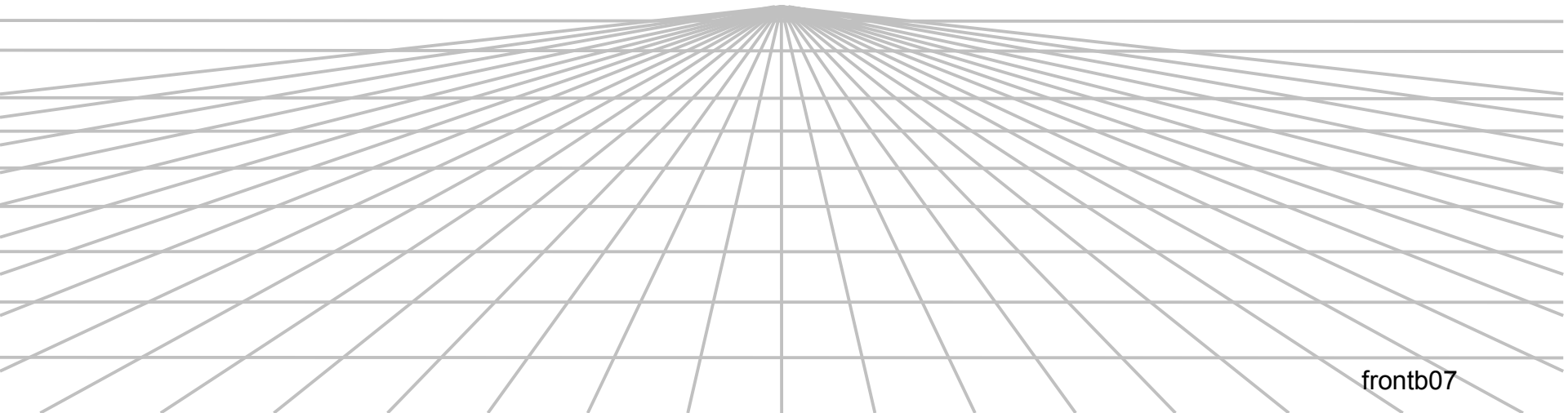
Initial analysis of gap between enterprise's

- Present level of security
- Where you need to get

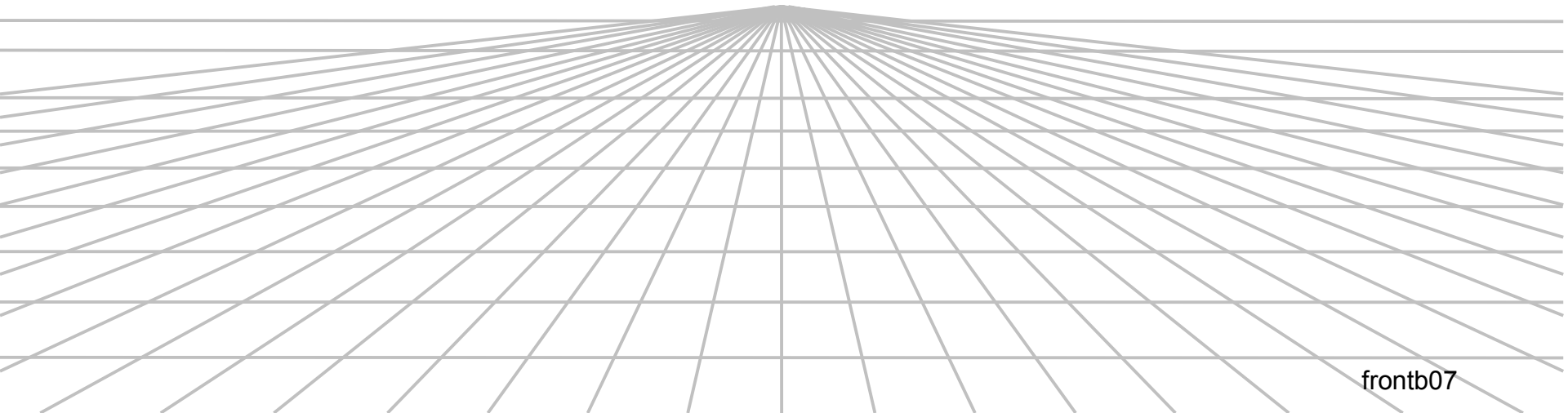
Security you need?

- Fundamentally a legal question, with these elements:
  - HIPAA statute
  - Regulations: the security matrix
  - State of art in the [defense] industry
    - » Encryption – PKI
    - » Access controls – biometrics
    - » Process controls
    - » Constant surveillance

Implementing What HIPAA Requires

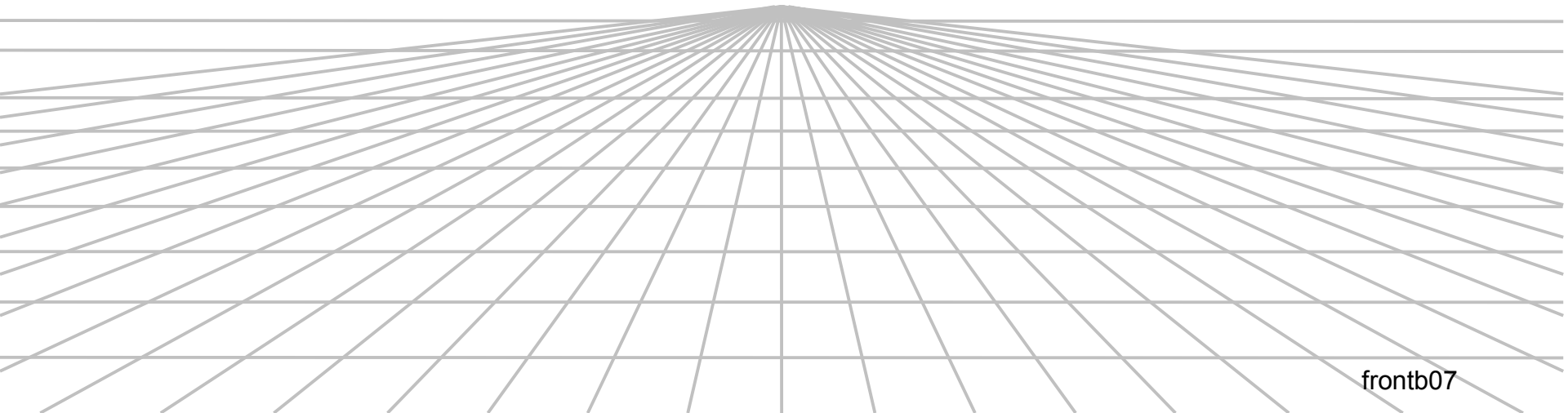


Personnel Security



frontb07

Biometrics



frontb07

HIPAA Security – Mandatory Choices

- ✓ All clinical systems
- ✓ Internal email
- ✓ Any communications systems carrying PHI (at any time)

  External email/Internet

    Physician consults

    Communications with patients

    Communications with payors

    Communications with regulatory authorities

HIPAA Security – Mandatory Choices

Function to be secured

+ Access
  - *Physical & personnel security (eg, nurses' stations)*
  - *Passwords +?*
  - *Biometrics?*
+ Transmission
  - PKI
+ Storage
  - PKI

Requirement for a Comprehensive, Effectively Implemented Plan

HIPAA itself

Business Judgement Rule
(applies to non-profits too)

Federal Sentencing Guidelines

Enterprise Compliance Plan for Information Security

Achieving a reasonable level of security is a multifaceted task

- Initial and on-going threat assessment (outside experts)
- Computer security
- Communications security
- Physical security: access to premises, equipment, people, data
- Personnel security
- Procedural (business process) security

Enterprise Compliance Plan

- ✓ Not simply and IT project
- ✓ Not only a compliance
- ✓ Will have a pervasive impact,
- ✓ [2] they will cost a great deal, and adverse impact on the delivery of care

Will the national security model Interfere will delivery of health care?

- ✓ Sheer cost

  legislative proposals

  **An unfunded mandate
- ✓ Business process change in the clinical setting – regime of surveillance and jeopardy
- ✓ Seeking legislative relief is inevitable

- ✓ HIPAA – Relationship of Security of EDI and Privacy
- ✓ Security is the infrastructure in which HIPAA's EDI and privacy rules are implemented (Plug-and-Play)
- ✓ On to EDI and privacy