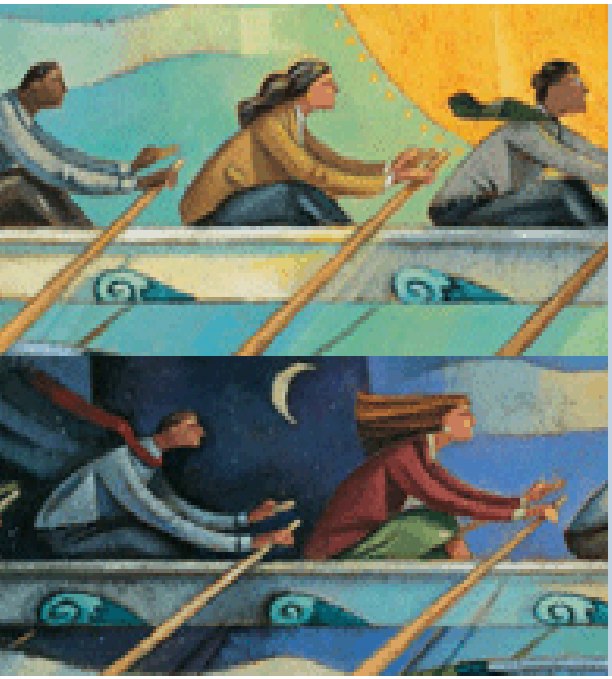
Eighth National HIPAA Summit



March 8, 2004

HIPAA Security Rule's Application to Employee Group Health Plans *Unique Problems and Compliance Strategies*

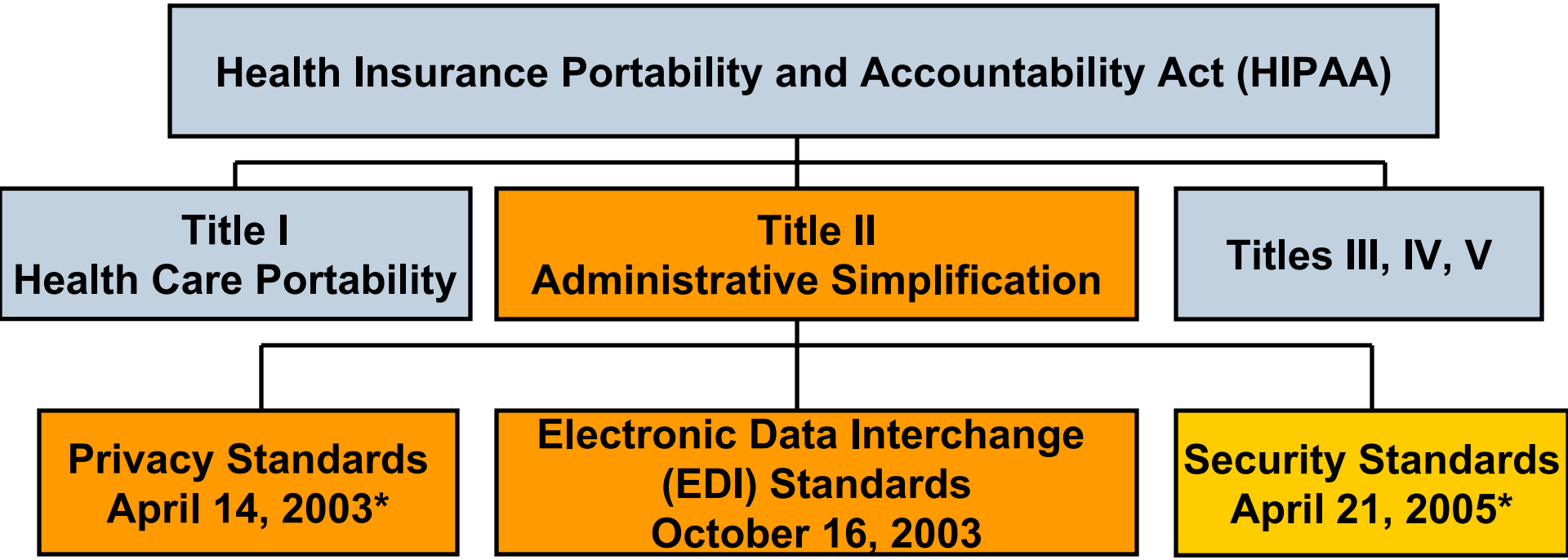
Mark Lutes – Epstein, Becker & Green
Bill Brossman – Mercer Human Resource Consulting

Session Agenda

- Security Rule's relationship to Privacy Rule
- HIPAA Security overview
- What employer plan sponsors must do
- Security risk assessment approaches for employers
- Sarbanes-Oxley as additional driver
- Parting thoughts/risk management themes
- Helpful references

Security Rule's Relationship to Privacy Rule

HIPAA Administrative Simplification



*** The effective date for small plans (i.e., those with less than $5M in receipts) is April 14, 2005 (privacy rules) and April 21, 2006 (security rules)**

Security Rule's Relationship to Privacy Rule

Privacy Standards – Quick Recap

- Privacy Standards require that Protected Health Information (PHI) be safeguarded, but primarily address:
  - Who can have access to PHI
  - How PHI can be used and disclosed
- Privacy Standards apply to *all PHI* regardless of whether oral, written, or electronic

HIPAA Security Overview
Scope of HIPAA Security Standards

- Privacy and Security are inextricably linked
  - Lack of adequate security safeguards increases risk of Privacy Standards violation
  - Both address how to control access and prevent unauthorized use or disclosure
- Security Standards protect only electronic PHI
  - Security Standards also address destruction or loss of e-PHI

HIPAA Security Overview

Broader *and* Narrower in its Application!

- ***Broader*** because it applies to all insured plans, not simply those that see more than summary and enrollment PHI
- ***Narrower*** insofar as it applies only to electronic PHI

HIPAA Security Overview
What is Electronic PHI (e-PHI)?

e-PHI **is PHI in electronic media, whether:**

- "At rest" in a storage device
  - For example, computer hard drive, disk, CD, and tape, or
- "In transit" via internet, dial-up lines, etc.
  - For example, e-mail, File Transfer Protocol (FTP), electronic data interchange (EDI), interactive voice response (IVR), and "fax back" systems that transmit PHI

HIPAA Security Overview
What is *not* Considered e-PHI?

- De-identified information
- PHI that was *not in electronic form* before transmission, for example:
  - Person-to-person telephone calls
  - Copy machines
  - Paper-to-paper fax machines
  - Voice mail

HIPAA Security Overview
Context for Employer Health Plans

- Employer performing plan administration functions is quasi-"business associate" for HIPAA purposes — employer security covenants reside in plan documents
- Could plan disclaim HIPAA Security responsibility on this theory — that the plan has no e-PHI — its business associates have it all? Unlikely…argument is probably too circular
- Moreover, plan's fiduciary needs would compel employer as administrator to examine and document plan IT security, plan sponsor's privacy and security rule; BA-type covenants also compel creation of a compliance program

HIPAA Security Overview
What e-PHI does Typical Employer Have?

Function	e-PHI
Customer Service & Claim Advocacy	E-mail, Imaging system
Claim Audit	Receipt of carrier claim tape
Data Analysis	Review of carrier claim data
Claim Appeals	E-mail, Imaging system
Enrollment and Disenrollment	E-mail, receipt and sending of eligibility enrollment from/to vendors

HIPAA Security Overview
HHS Framework

- 18 Security standards divided into six categories:
  - *administrative*,
  - *technical and physical safeguards,*
  - *organizational requirements,*
  - *policies and procedures, and*
  - *documentation*
- (Sound familiar? –already the general rule in privacy standards)

- Standards are given life through "implementation specifications"
- 13 specifications are "required" and 22 are "addressable" (see Exhibit A)

HIPAA Security Overview
What is the Difference?

- **"Required"** — not complicated — it must be met!!
- **"Addressable"** — you must implement it or document your assessment of why it is not a reasonable or appropriate safeguard for your environment
- If implementation specification is unreasonable or inappropriate, employer must implement equivalent alternative measure that is both reasonable and appropriate

HIPAA Security Overview
Administrative Safeguards Category

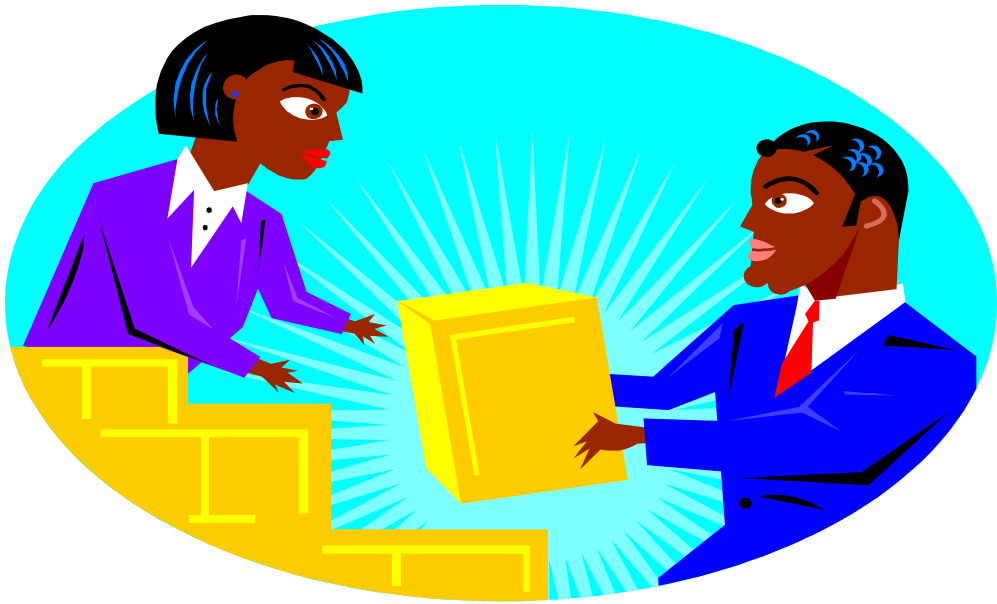
- Conduct risk analysis addressing confidentiality, integrity and availability ("CIA") of e-PHI
- Implement measures to reduce identified risks to appropriate levels
- Apply sanctions to workforce members who fail to comply with procedures
- Regularly review IS system activity – audit logs, access reports, security incident reports
- Assign someone security responsibility for policies and procedures
- Implement policies regarding workforce security
- Develop (addressable) procedures to document, review and modify access privileges

HIPAA Security Overview
Policy and Procedure Documentation

- Implement and update reasonable and appropriate policies and procedures
- Maintain in written or electronic form and retain for 6 years
- Make available to persons responsible to implement
- Update for operational change
- Obtain HR/IT collaboration

HIPAA Security Overview
Physical Safeguards

- Facility access controls — implement policies and procedures limiting access
- Access control and validation procedures
- Maintenance records-repairs and modifications to hardware, doors, locks
- Facility security plan
- Workstation controls
- Device and media controls



HIPAA Security Overview
Technical Safeguards

- Unique user identification (required)
- Emergency access (required)
- Automatic log-off (addressable)
- Encryption and decryption (addressable)
- Audit controls-hardware, software or procedures that record and examine system activity
- Policies to protect data integrity
- Electronic mechanism to corroborate that data has not been altered or destroyed
- Person or entity authentication

HIPAA Security Overview
In Theory, Burden is on ERISA Plan

- … but it may not matter because plan, not employer, is covered entity
- In privacy context, employer is quasi-business associate
  - Employer certifies to plan that it will use PHI only for plan administrative purposes, report breaches, return or destroy PHI when done

What Employer Plan Sponsors Must Do
Security Infrastructure Requirements

Security Rules parallel Privacy Rules. Plans are required to:

- Appoint Security Official
- Conduct Security risk assessment
- Develop written policies and procedures
- Train staff and impose sanctions on violators
- Require contractual compliance by Business Associates

What Employer Plan Sponsors Must Do
Amend Plan Documents and Secure Systems

In most cases, employer plan sponsors must amend plan documents and secure their systems:

- Like Privacy, Security Rule requires employers with access to e-PHI to:
  - amend plan documents, and
  - promise to secure e-PHI
- Security rules *exempt* employer from having to amend plan documents if employer only receives e-PHI that is:
  - Summary health information and/or
  - Enrollment and disenrollment information
- e-PHI may be disclosed to employers only if employer promises to secure it

What Employer Plan Sponsors Must Do
Secure Eligibility and Enrollment Data?

- Securing eligibility and enrollment data is situational
  - If employer receives e-PHI (e.g., information relating to claims appeals, auditing or customer service) . . .
  - Then employer may need to secure *all e-PHI* "created, received, maintained, or transmitted" to or by employer on behalf of plan
- Important difference from HIPAA Privacy Rule

What Employer Plan Sponsors Must Do
Workforce Training

Implement security awareness and training program

- Training activities might include:
  - Issue periodic security reminders
  - Train staff to use virus protection
  - Train staff to use and update security passwords
  - Train staff in procedures to monitor login attempts and report discrepancies

What Employer Plan Sponsors Must Do
Business Associate (BA) Agreements

- Ensure that BAs contractually commit vendor to Security compliance
- BAs and their agents and subcontractors who use e-PHI must also adhere to Security Standards
  - BAs must report security incidents they are aware of to Covered Entity
  - BA services can be terminated by Covered Entity for violations
- Requires revisiting BA agreements for HIPAA Security Compliance
- HHS may develop sample contract language

Security Risk Assessment Approaches
Fundamental Role of Risk Assessment

- The bad news:
  - Compliance is impossible without thorough documented risk assessment
  - Accurate and thorough assessment expressly required by Security Rule and must be periodically updated
- The good news:
  - Plan is not expected to eliminate all security risk — only to understand it and reduce it to what it deems to be an acceptable level

Security Risk Assessment Approaches
Privacy Rule Data Flow Analysis Should be Starting Point

- Identify potential risks and vulnerabilities to confidentiality, integrity, and availability of e-PHI
- Consider size, complexity, technical infrastructure, costs of security measures and probability and criticality of e-PHI risks
  - Based on risks identified, decide how and (if applicable) whether to implement additional administrative, physical, and technical safeguards
- ERISA plan must respond to each risk but can use flexible approach
- Plan might also use a third party evaluation (suggests efficacy of accreditation, e.g., URAC)

Security Risk Assessment Approaches
Dilemma for e-PHI Security — What Methodology?

- Quantitative analysis:
  - Attempts to assign objective numerical values to components of risk and loss
  - Difficult to assess dollar estimate of loss expectancy related to each threat where primary asset is e-PHI
- Qualitative approach:
  - Can proceed from threat listing
  - Assets requiring protection can be assigned exposure levels relative to each threat

Security Risk Assessment Approaches
Practical Risk Analysis for e-PHI

- Our opinion/experience — use a modified qualitative approach
  - Identify all e-PHI containing systems and applications
  - Identify threats/vulnerabilities
  - Assign level of acceptable risk
  - Select safeguards to mitigate risk to acceptable levels
  - Get input from a variety of client sources (IT, benefits, and physical security)
- In doing so, we use quantitative methodologies to evaluate data but fundamentally it is qualitative in nature
  - No attempt to assign specific dollar values to the threats – employer's prioritization directs risk management

Security Risk Assessment Approaches
Grand Dialectic

- Understand it to avoid financial consequences
- Rule built on complementary processes of risk analysis and risk management
- “Process is as important as product”
  - Drives our documentation approach
- Health plan not expected to eliminate all security risk but is expected to reduce to acceptable level
  - This presents traps and opportunities
  - How you proceed will dictate need for future expenditures

Security Risk Assessment Approaches
Example – IT Threat Evaluation

- For each e-PHI repository, assess likelihood that threatened event will occur. For example:
  - *"Not applicable"* – internet hacking of a stand-alone desktop database
  - *"Unlikely to happen"* – earthquake in Northeast
  - *"Has happened, expect to happen again"* – earthquake in Los Angeles region
  - *"Could happen"* – accidental file deletion
- In assessing threat likelihood, account for existing mitigation factors, such as firewalls or other safeguards already in place
- For each threat being evaluated, rank employer cost if threatened even actually occurs, e.g., negligible, low, medium and high
  - Employer can assign dollar ranges to each cost category

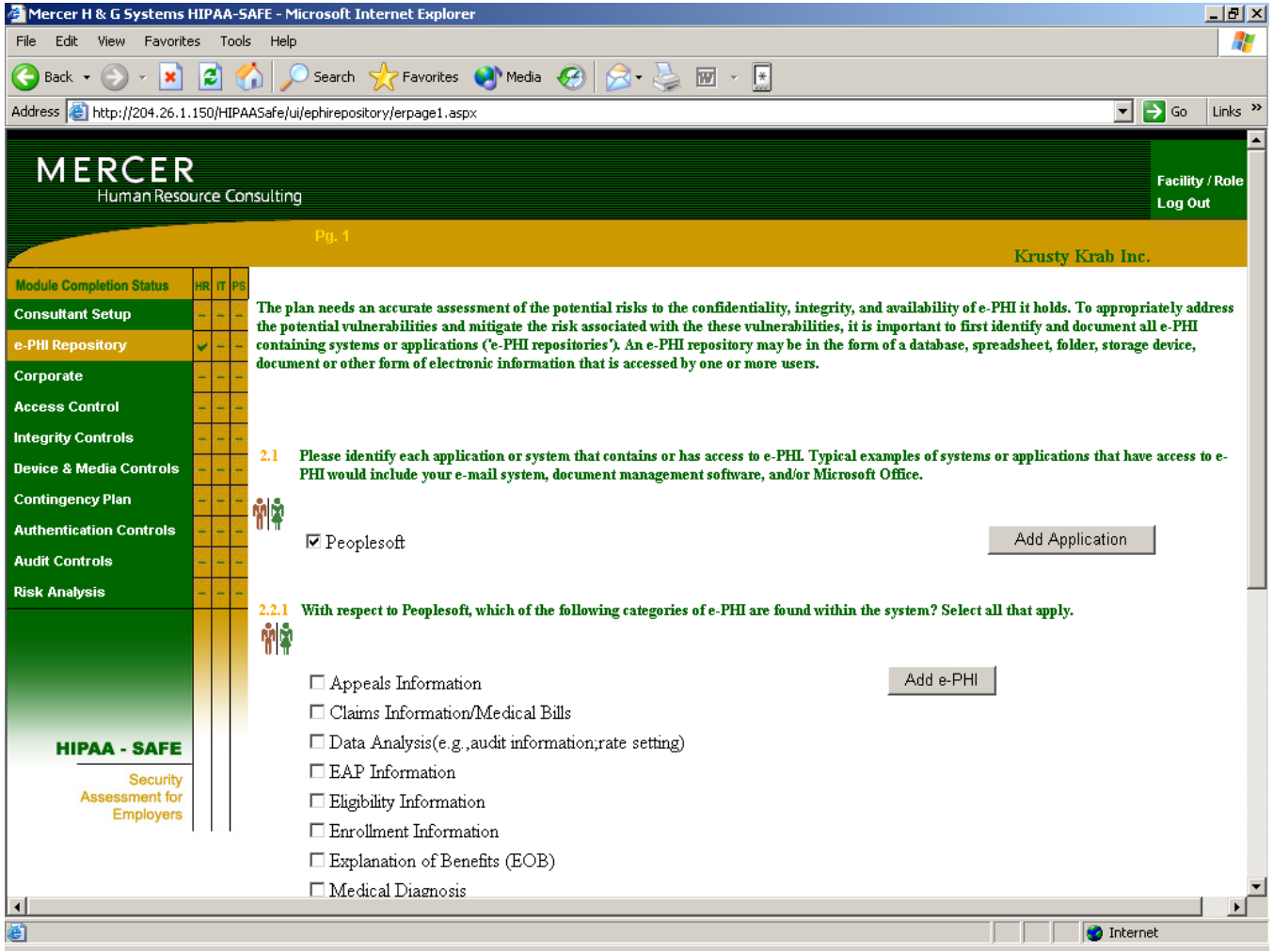
Security Risk Assessment Approaches
Example – HR Threat Evaluation

- HR survey participants evaluate threat to e-PHI from two different perspectives
  - Cost to employer if e-PHI is lost or destroyed due to occurrence of threat
  - Cost to employer resulting in unauthorized disclosure of e-PHI due to occurrence of threat
- To evaluate risks associated with e-PHI loss, consider timing and expense of replacement. For example:
  - Redundant data (e.g., e-PHI that is backed up or held in duplicate by vendor and that can be obtained quickly and inexpensively will mitigate cost of loss or destruction)
  - e-PHI that cannot be quickly and inexpensively retrieved or reproduced would be of higher cost if destroyed due to occurrence of threatened event

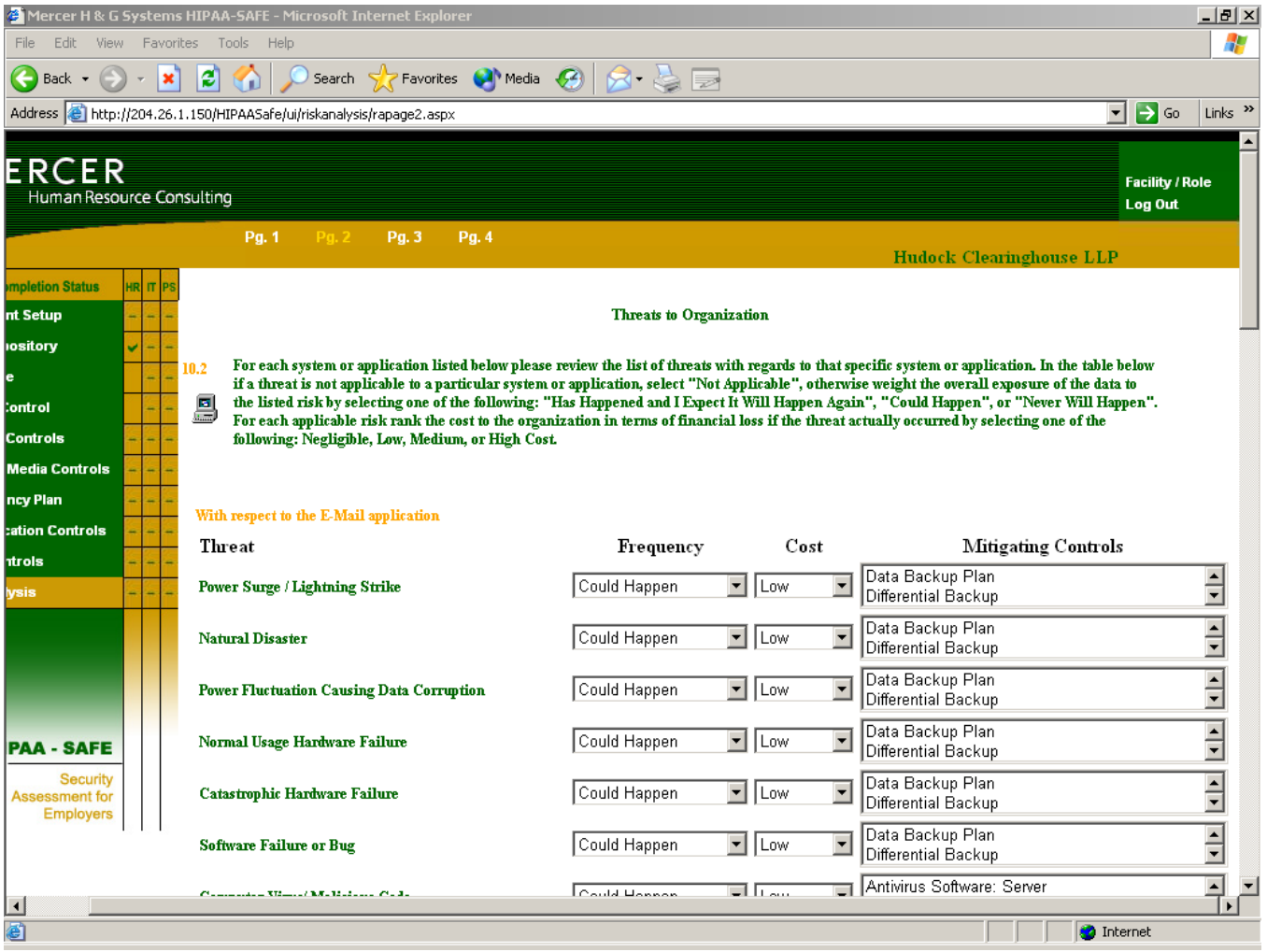
Security Risk Assessment Approaches
Example – HR Threat Evaluation – Cost of Data Loss

- When evaluating cost relating to unauthorized disclosures of e-PHI, consider sensitivity of information. For example:
  - *"Negligible"* – disclosure concerns employee's plan eligibility status
  - *"Low"* – disclosure concerns plan's claim payment of $300 to employee, but no diagnosis or treatment information
  - *"Medium"* – disclosure of plan's dental records
  - *"High"* – disclosure concerns employee's treatment for substance abuse, mental health, or HIV status

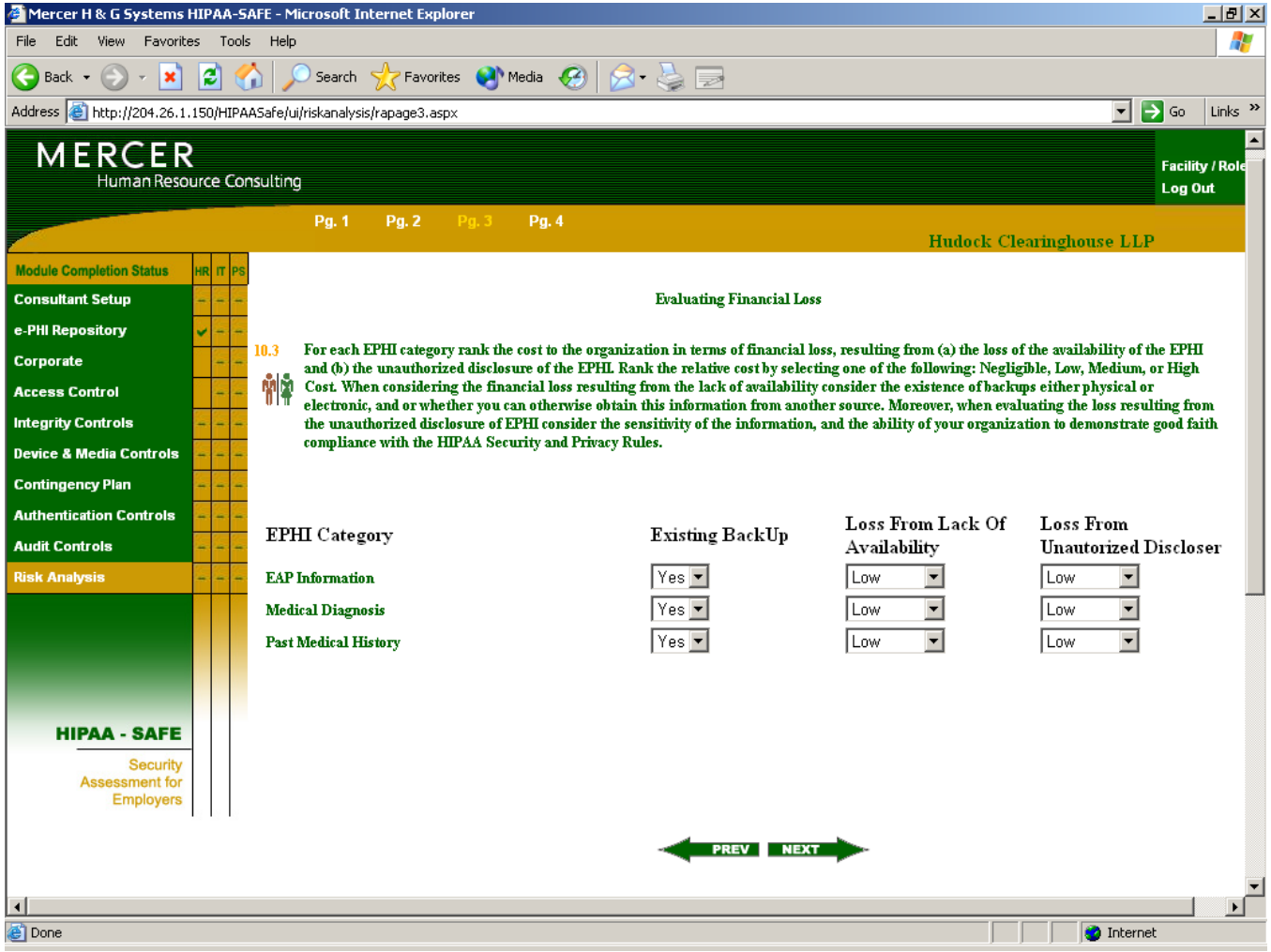
Security Risk Assessment Approaches
HIPAA Safe Screen Shots



Security Risk Assessment Approaches
HIPAA Safe Screen Shots



Security Risk Assessment Approaches
HIPAA Safe Screen Shots



Sarbanes Oxley as Additional Driver
Risk Analysis and Documentation

- Sarbanes Oxley was intended to increase transparency and reliability of reports filed with SEC by public companies and relied upon by investors
- However its lessons reach privately held business corporations and nonprofits as well through application of its standards by:
  - state attorneys general
  - D&O and E&O insurers
  - Lenders
  - auditors

Sarbanes Oxley as Additional Driver

CEOs and CFOs required to annually certify

- Officers must certify they have designed internal financial and “disclosure controls” and have evaluated their effectiveness within 90 days
- Experts agree that disclosure controls necessarily implicate regulatory compliance including privacy and security
- Failure to make certifications carries civil and criminal liability
- Parallels Sentencing Guidelines in creating imperative toward documented diligence and audits

Parting Thoughts/Risk Management Themes
"Security not Fundamentally about Technology"

- Security is about risk assessment and applying policy, procedure and some technology to address those risks
- Task is to document ERISA plan's priorities and to make sure there is evidence of current diligence
- Task also is to marshal external validators for decisions health plan has made

Parting Thoughts/Risk Management Themes

Industry "Misspends" when it applies Technology to Modest Risks …

- Do not presume this will require more money…presume it will require conceptualization and new documentation
- Learn what effective compliance programs involve!
- Institute "controls" (Sarbanes Oxley's theme)
- Install procedures for periodic diligence and monitoring (Sentencing Guidelines)

Parting Thoughts/Risk Management Themes
Components of Solution

- Challenge is to develop cost effective solution for employee benefit plan environment
- Participants in compliance solution: employer as plan administrator, TPA, insurer
- Solution needs to integrate benefits and IT personnel in assessment and risk management program

Helpful References

To learn more about Security Rules:

- Security Regulations are available at: http://aspe.os.dhhs.gov/admnsimp/FINAL/FR03-8334.pdf
- United States Department of Health and Human Services Health Care Administrative Simplification Website: http://aspe.os.dhhs.gov/admnsimp/
- For a glossary of terms and definitions, see the Security Rule definitions sections at 42 CFR §160.103, §164.103, and §164.304

Exhibit A: Security Rule
Standards and Implementation Specifications

Standards	42 CFR	Implementation Specification (R)=Required, (A)=Addressable	
Administrative Safeguards			
Security Management Process	164.308(a)(1)	Risk Analysis (R) Sanction Policy (R)	Risk Management (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	Security Official (R)	
Workforce Security	164.308(a)(3)	Authorization/Supervision (A) Termination Procedures (A)	Workforce Clearance Procedure (A)
Information Access Management	164.308(a)(4)	Isolating Clearinghouse Function (R) Access Authorization (A)	Access Establishment & Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Log-in Monitoring (A)	Protection from Malicious Software (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response & Reporting (R)	
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Emergency Mode Operation Plan (R) Applications & Data Criticality Analysis (A)	Disaster Recovery Plan (R) Testing & Revision Procedure (A)
Evaluation	164.308(a)(8)	Periodic Technical & Non-Technical Evaluation (R)	
Business Associate Contracts	164.308(b)(1)	Written Contract or Other Arrangement (R)	

Exhibit A: Security Rule
Standards and Implementation Specifications

Standards	42 CFR	Implementation Specification (R)=Required, (A)=Addressable	
Physical Safeguards			
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Access Control and Validation Procedures (A)	Facility Security Plan (A) Maintenance Records (A)
Workstation Use	164.310(b)	Policies and Procedures re: Functions and Attributes (R)	
Workstation Security	164.310(c)	Physical Safeguards (R)	
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R)	Accountability (A) Data Backup and Storage (A)
Technical Safeguards			
Access Control	164.312(a)(1)	Unique User Identification (R) Automatic Logoff (A)	Emergency Access Procedure (R) Encryption and Decryption (A)
Audit Controls	164.312(b)	Hardware, Software, or Procedures to Record and Examine Activity (R)	
Integrity	164.312(c)(1)	Mechanism to Authenticate *e-PHI* (A)	
Person or Entity Authentication	164.312(d)	Procedures to Verify a Person or Entity Seeking Access (R)	
Transmission Security	164.312(e)(1)	Integrity Controls (A)	Encryption (A)