HIPAA - - Basic Concepts and Implementation Roadmap

Prepared by:

SEYFARTH ATTORNEYS SHAW

David Weiner dweiner@seyfarth.com

Fredric Singerman fsingerman@dc.seyfarth.com

Today's Agenda

- Introduction of HIPAA Privacy and Electronic Transaction Rules
- Simplification of complex compliance concepts
- Step-by-step compliance plan
- Review of common issues

Workshop Materials

- Presentation screens
- Project Plan
- Computer-based training screens

What We Are Not Covering

- Your “provider” (pharmacy) duties
- Electronic transactions in detail

HIPAA Basics

- Privacy of medical information
- Electronic transactions
- Security and electronic signatures *(not final)*

HIPAA Privacy Basics

- HIPAA imposes duties on “covered entities” and their business associates who receive, transmit or use “protected health information”
- An employer has “covered entity” duties as health plan sponsor/administrator
- HIPAA duties cover privacy of protected health information and its electronic transmission between covered entities

Effective Dates

- Privacy regulations - April 14, 2003
  - Small plan exception extends deadline to April14, 2004 for plans not in excess of $5 million annually
  - Same delayed effective date for existing business associate contracts
- Electronic transactions - October 16, 2003*
  - * Compliance plan due October 15, 2002

Penalties for Non-Compliance

- Civil Penalties
  - $100 per violation, up to $25,000 per person, per year
- Criminal penalties
- Possible civil litigation (under state law)

HIPAA Definitions
Covered Entities

- Health Plans
  - Employer sponsored plans
  - Some insurance companies
  - HMOs
- Health care providers that conduct specific transactions electronically
- Clearinghouses

HIPAA Definitions
Employer Health Plans

Covered

- ☑ Medical Plans
- ☑ Dental Plans
- ☑ Health Flexible Spending Accounts
- ☑ Retiree Medical Plans
- ☑ ERISA covered Employee Assistance Plans

HIPAA Definitions
Health Plans

Not Covered

- ☒ Workers' Compensation
- ☒ Disability Plans
- ☒ Stop loss
- ☒ Accident Plans
- ☒ Non-ERISA covered Employee Assistance Plans
- ☒ Life Insurance Plans

HIPAA Definitions
Protected Health Information

- Relates to an individual's past, present or future
  - physical or mental health or condition;
  - payment for health care; or
  - provision of health care.
- Identifies or could identify the individual

Where Does Employer/Plan Sponsor Receive, Transmit or Use PHI?

- Request for payment from health care provider/claims processing
- Inquiry from participant regarding eligibility or coverage/help desk function
- Coordination of benefits/subrogation
- Utilization review/underwriting

Business Is Not Over

- HIPAA Privacy will change some of what you do (or the way you do it)

BUT

- It permits many Plan activities to continue; others require authorizations or procedures to be maintained

Permitted Uses and Disclosures of Protected Health Information

- To the individual
- With “consent” or “authorization”
- For “treatment, payment or health care operations” (TPO), *but limited to the “minimum necessary” PHI*
- HHS/Public policy disclosures
- “De-identified” disclosures

Using and Disclosing PHI for “TPO”

- Payment and health care operations cover most activities of a health plan
- Policies/Plans must reflect
- Minimum necessary rule applies
- No authorization required

Payment and Operations

- *Payment* -- Day-to-day administration
- *Operations* – Global management activities

Payment

- Determining eligibility or coverage
- Risk underwriting
- Billing and claims management
- Pre-authorization and utilization
- Reviewing medical necessity
- Obtaining payment from stop-loss insurer
- Disclosure to a consumer reporting agency

Health Care Operations

- General administration
- Quality assessment or review
- Obtaining legal services, audits, etc.
- Securing stop-loss insurance
- Due diligence in health plan mergers

“Minimum Necessary” Requirement

- Must limit the use or disclosure to the minimum necessary to accomplish purpose
- “Reasonable effort” standard
- Does not apply to:
  - Communications with health care provider for treatment
  - Disclosures to the individual
  - Disclosures required by law

Minimum Necessary

- Can you do it with less information?
- Can you do it with fewer people accessing the information?

Minimum Necessary *Uses*

- Must identify who needs access
- Must identify information and conditions of access
- Must make reasonable efforts to limit to above

Routine Versus Non-Routine *Disclosures*

- If routine, must implement policies and procedures (or protocols) to limit to minimum necessary
- If non-routine, must develop criteria designed to limit and use them to evaluate requests

Payments and Operations Illustrated

- Sending eligibility information to Third Party Administrator
- Following up on Executive Vice President’s claim
- Reviewing activities of high-volume providers
- Accessing claims information for budgeting

HIPAA Privacy
Permitted Disclosures To Sponsor

- Information necessary to carry out plan administrator functions
  - Not plan sponsor functions
  - Limited to plan personnel
- Summary health information for:
  - obtaining insurance bids
  - amending or terminating the plan

Use or Disclosure Checklist

- Is it payment or operations?
- Is it minimum necessary?

⇨ **If both answers are “yes,” proceed without authorization**

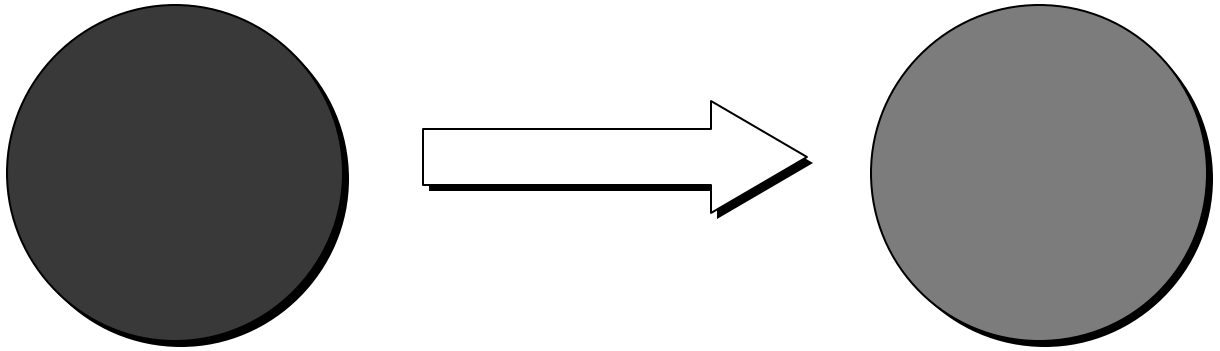
HIPAA Privacy
Judicial and Administrative Proceedings

- Permitted to disclose protected health information in response to a judicial or administrative order
- Permitted to disclose protected health information in response to a subpoena, discovery or other legal process if requesting party used reasonable efforts to notify affected party or secure a protective order

HIPAA Privacy
Rights of Individuals

- Right to a Privacy Notice
- Right to review and amend protected health information
- Right to an accounting of protected health information
- Right to request additional restrictions on use or delivery of protected health information
  - Privacy
  - Confidentiality

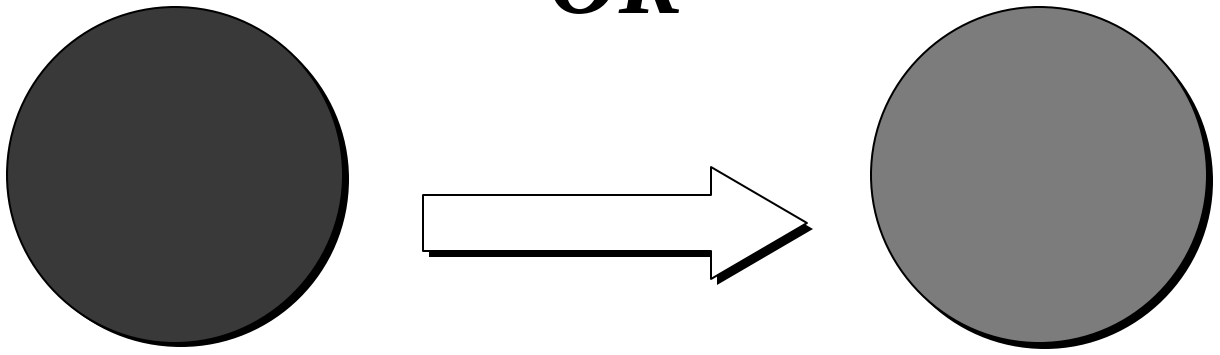
Disclosure of PHI



Medical Plan

Disability Plan

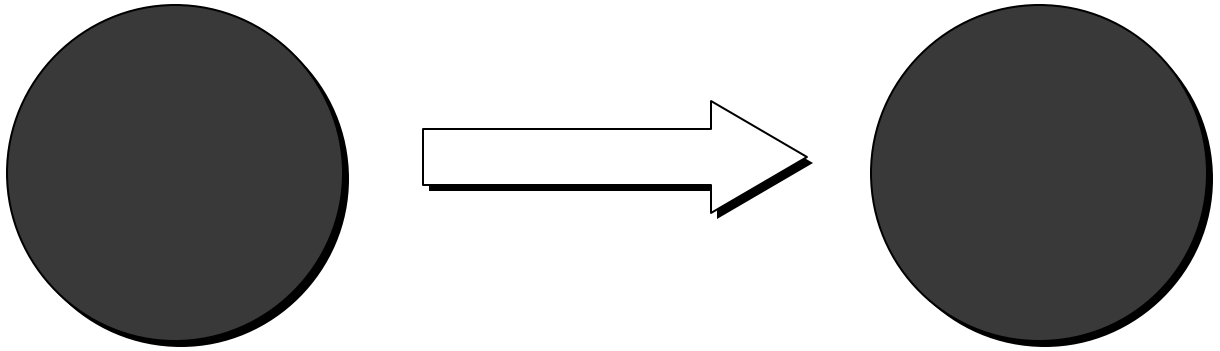
OR



Medical Plan

Employer

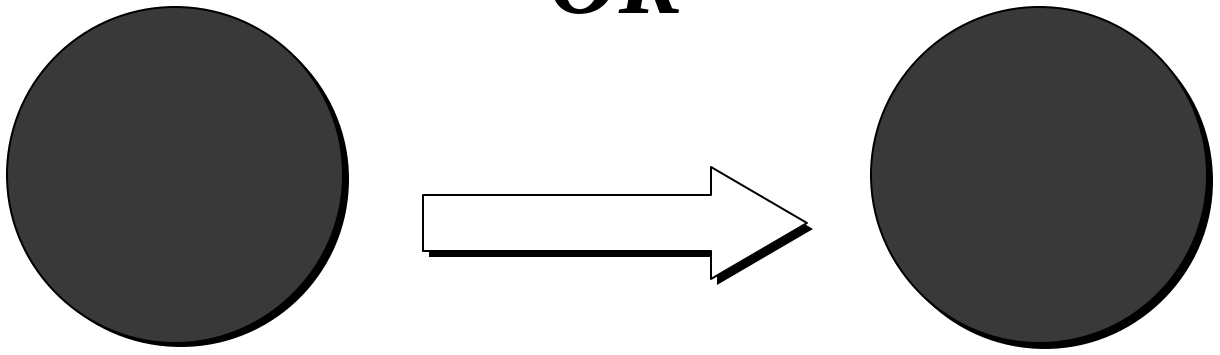
Disclosure of PHI



Medical Plan

Dental Plan

OR



Medical Plan

HRA

HIPAA's Impact

- Covered Plans ➜ Not Covered Entities = Minimum necessary for treatment, payment or operations purposes or pursuant to authorization
- Covered Plans ➜ Plan Sponsor (for plan administrative functions) = Minimum necessary and a plan amendment
- Covered Plans ➜ Covered Entities = Minimum necessary for treatment, payment or operations
- Not Covered Entities ➜ Covered Plans = HIPAA does not apply

HIPAA's Impact

Before HIPAA

- An employee responsible for the medical plan could disclose all of a participant's protected health information to an employee responsible for the dental plan for purposes of coordination of benefits

After HIPAA

- Only the minimum necessary may be disclosed

HIPAA's Impact

Before HIPAA

- An employee in the Accounting Department could request protected health information from the medical plan to try to cut company costs.

After HIPAA

- Only summary health information may be disclosed.

HIPAA's Impact

Before HIPAA

- An employee working on medical plan fraud could share protected health information with an employee working on disability plan fraud

After HIPAA

- An authorization is necessary to share medical protected health information with disability plan

HIPAA's Impact

Before HIPAA

- An employee working on disability claims could share protected health information with an employee working on workers' compensation claims or medical claims

After HIPAA

- No change

Business Associates

- Not members of covered entity's workforce
- Receive or create protected health information

Business Associates Compliance

- Covered entity receives satisfactory assurance
- Business associates contract provisions
  - Uses and disclosures
  - Confirmation of compliance
  - Cooperation in compliance
  - Privacy breaches

Responsibility for Violations by Business Associates

- Knowledge of a “pattern or practice” of violations
- Must take reasonable steps to correct
- If reasonable steps unsuccessful, must either:
  - Terminate contract, or
  - Report problem to HHS

Required Actions for Breaches

- Mitigation of breach
- Sanctions against breacher
- No retaliation against complainer

HIPAA Electronic Transactions

Electronic Transaction Basics

- Health Plans and other Covered Entities will need to use uniform codes and formats when electronically transmitting certain health information
- HIPAA standardizes the hundreds of different formats and codes
- Of less importance if administration outsourced

Electronic Transaction Basics

Electronic Media

- Includes transmissions through the internet, extranet, leased lines, dial up lines, private networks and those transmissions moved from one location to another using magnetic tape, disk or compact disk media
- It does not include fax imaging or voice response

Electronic Transaction Basics

Three Step process:

- Is the transaction covered by HIPAA?
- Is the Health Plan or its business associate, performing the transaction?
- Does the definition of the transaction require a health plan (or other Covered Entity) on one or both sides of the transaction?

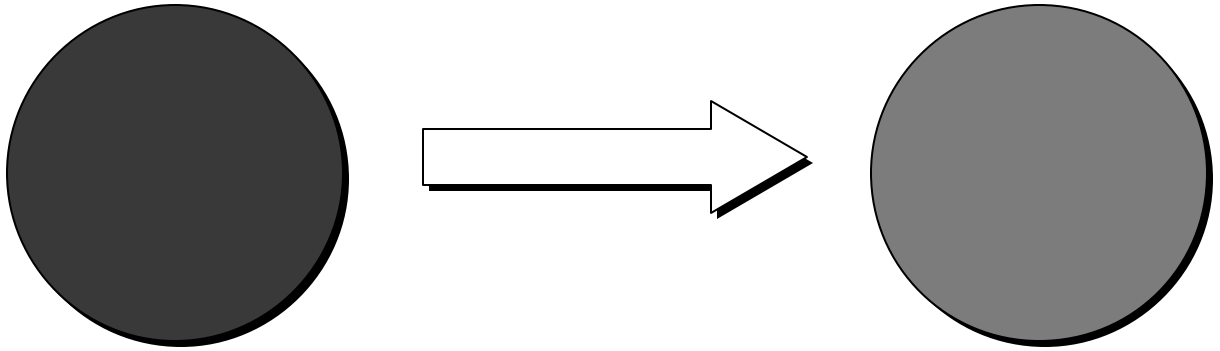
Electronic Transactions

- Health care claims or equivalent encounter information
- Eligibility for Health Plan
- Referral certification and authorization
- Health care claim status

Electronic Transactions

- Enrollment and disenrollment
- Health care payment and remittance advice
- Health Plan premium payments
- Coordination of benefits

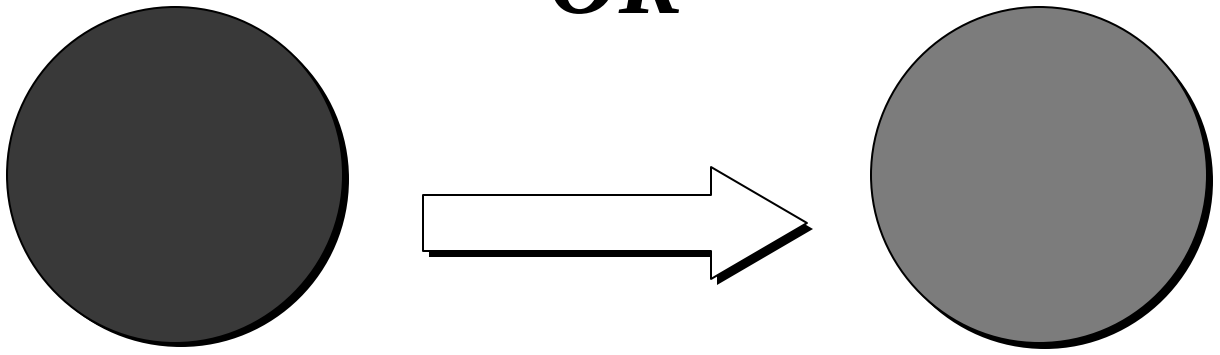
Electronic Transactions



Medical Plan

TPA

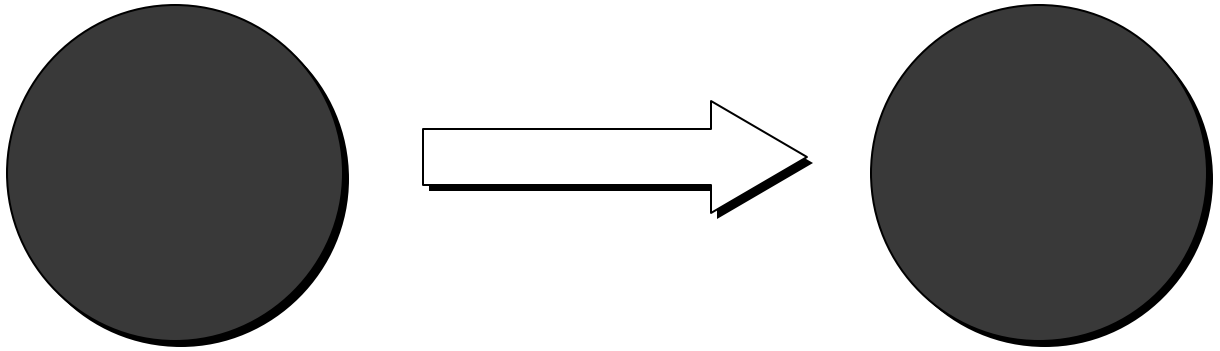
OR



Medical Plan

Employer

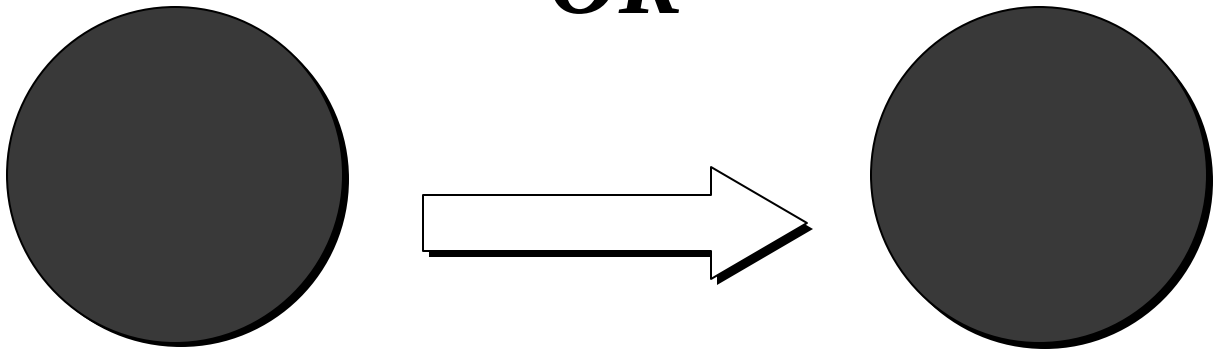
Electronic Transactions



Medical Plan

Provider

OR



Medical Plan

Other Plan

Implementation and Project Overview

Factors Affecting Compliance

- Insured or self-insured?
- Degree of outsourcing
- Health plan locations

Project Objectives

- Identify compliance gaps
- Address procedural items
- Address substantive items

Procedural

- Are policies written?
- Are plans amended?
- Are authorizations in shape?
- Are business associates contracts sufficient?

Substantive

- Do you need to limit personnel?
- Do you need to limit information?
- Do you need to enhance security?

Steps for Implementation

- Appoint a privacy officer
- Implement protocols to assure adequate separations
- Develop policies and procedures
- Train employees
- Amend plan documents
- Amend Business Associates Contracts
- Create and distribute Privacy Notice

Appoint Privacy Officer

- Appointment of privacy and compliance officers
  - receiving complaints regarding violations
  - receiving requests for access to information
  - receiving requests to amend
  - receiving requests for accounting of disclosures

Provide Adequate Separations

- Restrict access to designated employees or other persons under sponsor's control
- Restrict use to plan administrative functions
- Assure "minimum necessary"
- Create a mechanism for resolving complaints and compliance issues
- Document Protocols and Procedures

Document Policies & Procedures

- Impose limitations on use of and access to protected health information
- Create complaint resolution procedures
- Impose sanctions for violations
- Create a policy against reprisal/intimidation
- Provide for individual rights to accounting, review, amend, etc.

Training of Employees

- Train employees on company policies and sanctions for failure to comply
- Best approach will be determined based on how much is needed for the specific individual; how many people need to be trained; how hard it is to document training; how often people and policies change

Plan Documents

- Specify permitted employees
- Restrict use and disclosure by plan sponsor
- Require employer certification

Business Associates Contracts

- Compliance assurances and cooperation
- Report improper uses or disclosures
- Termination provisions
- Return or destruction of documents

Privacy Notice

- Specific “core-elements” must be addressed:
  - Permitted uses of information
  - Individuals’ rights
  - Covered entity’s duties
  - Complaints

Project Overview
Assessment

- Determine scope of activity
  - identify covered plans
  - identify sources of protected health information to plan
  - identify business associates
- Track the flow of protected health information
  - routine third party transactions
  - flow between Corporate Benefits and business associates
  - flow between retail locations and Corporate Benefits

Project Overview
Assessment

- Draw Health Plan “firewall”
  - Corporate Benefits
  - Human Resources (HR)
  - Store personnel
- Review plan documents, business associates agreements, etc.
- Evaluate electronic transactions
- Prepare an assessment/gap analysis report

Project Overview
Policies and Procedures

- Assess and document use of minimum necessary PHI in routine Plan transactions
- Draft policies and procedures manual
- Get Buy-in from Corporate Benefits, HR and legal
- Use these policies and procedures as the basis of your training program

Project Overview
Contracts and Plan Documents

- Amend contracts with HMOs, PPOs and other Covered Entities
- Amend contracts with TPAs and other Business Associates
- Amend plan documents and summary plan descriptions

Project Overview
Forms and Disclosure

- Authorization forms
- Revocation of Authorization Forms
- Appointment of personal representative
- Privacy notice

Project Overview
Training

- Identify which employees will need training
- Determine whether to train outside firewall
- Finish initial training by effective date
- Train new hires about privacy
- Document training

Computer-Based Training Screens

- See Tab 3

Project Overview
On-Going Compliance

- A health plan must audit its privacy practices and procedures
- Determine what you will need to review; who will accomplish; how often

Common Issues

- State privacy restrictions
- Firewall design
- Spouse/dependent issues
- Interaction with claims rules

State Privacy Restrictions

- Do they apply to self-insured plan?
- Can they be source of liability?
- How do I determine “more restrictive?”

Firewall Design

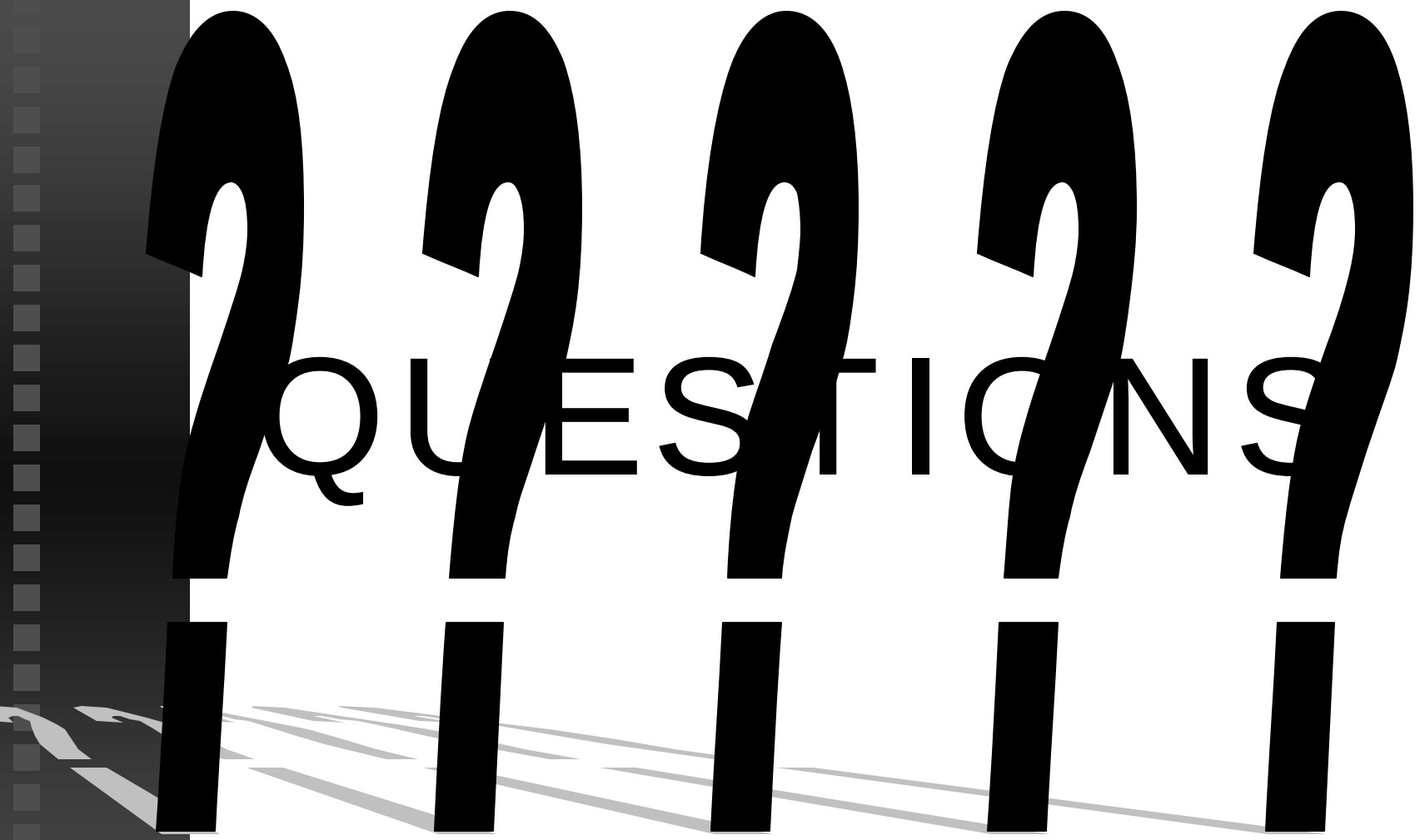
- What is recommended analysis for considering who is inside and outside?
- Should I train anyone outside firewall?
- Can I enter business associates contracts with employee outside firewall?

Spouse/Dependent Issues

- Can I share employee protected health information with spouse or vice versa?
- Can I share minor dependent protected health information with parent or step-parent?

HIPAA versus Claims

- Will required claims responses satisfy HIPAA?
- Will a personal representative for claims purposes be authorized to see protected health information for HIPAA purposes?



Presented by:

Seyfarth Shaw

Fredric S. Singerman
David M. Weiner