HIPAA Loss Prevention and Business Associates: A Risk Management Perspective

October 26, 2001

Alan M. Reisch
areisch@goulstonstorrs.com
Steven J. Snyder, Esq.
ssnyder@goulstonstorrs.com

goulston&storrs
thinkresults

HIPAA and Risk Management Themes to Remember

- HIPAA risks are not new risks
- Business Associates can be used to manage some HIPAA risks
- Insurance may not be available
- HIPAA is a roadmap for risk management

Topics For Today

- What is Risk Management and How Is It Done?
- HIPAA Risks for Covered Entities and Business Associates
- HIPAA as a Tool for Risk Management

What is Risk Management and How Is It Done?

- What is Risk?
  - Exposure to something that is uncertain - that may cause you harm.
- Risk Acceptance v. Risk Aversion
  - Businesses, just like people, can either accept risk comfortably, be manifestly risk averse, or fit elsewhere on the continuum
- At some point, Risk must be MANAGED

So, What is Risk Management?

- A Process of Identifying, Understanding and Handling Risk
  - What is the Risk?
  - Who is Affected by the Risk?
  - Can the Risk be Managed and, if so, How?
- What is the Risk?
  - In the Context of Risks such as HIPAA Risks, There is really nothing new

There's Really Nothing New

- Just Think of Where We've Already Been
  - Asbestosis Exposures
  - Environmental Exposures
  - Lead Paint Exposures
  - Tobacco
  - Guns (and Roses)
  - Mold

And Consider This

- **There was the World Before September 11, and There is the World After September 11**
- **We're Now Dealing Daily With:**
  - Consideration of the Total Loss of Massive Structures
  - Business Interruption, and Contingent Business Interruption, Lasting for a Long Time and Impacts a Large Area, or Many Areas ALL AT ONCE
  - Bio-Hazards that are Intentionally Introduced
  - Questions of How Risk Strategies Premised on Exposures that are Fortuitous Can be Dealt With When Harm is Intentional

And Then There's HIPAA

- **In Many Ways, Even in the Context of HIPAA, There's Nothing New**
  - **Breach of Confidentiality Has Always Led to Potential Exposure**
  - **Tension Between Information Needed to Diagnose, Treat and Manage v. Protection of Privacy Has Always Been Present**
- **But, the Issue is Now Crystallized**

HIPAA IS:

- An Objective Manifestation of a Perceived Social Good
- A State of Mind
- A Paradigm Shift
- The Essence of a Standard Against Which You Will Be Judged
- **And the Risk Is:**

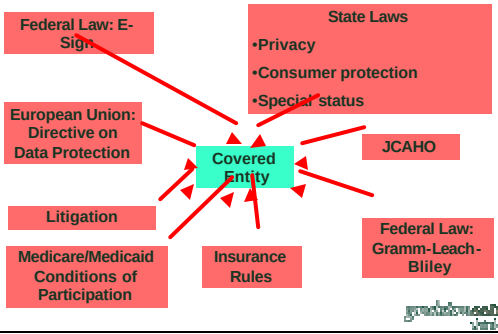
THE UNAUTHORIZED DISCLOSURE OF PROTECTED HEALTH INFORMATION

- Which Can Lead to:
  - Civil Penalties
  - Criminal Penalties
  - Litigation by Individuals
  - Litigation by Other Providers

HIPAA Worries and HIPAA Risks

- Privacy and Security Before HIPAA
- Scope of HIPAA
- The Six Things Every Covered Entity Should Worry About Under HIPAA
- What is a Business Associate?
- The Three Things Every Business Associate Should Worry About Under HIPAA
- Using Business Associates to Manage Risks

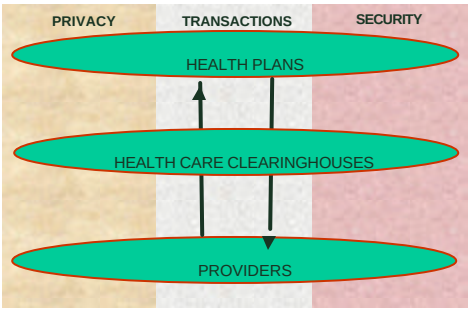
Non-HIPAA Privacy and Security



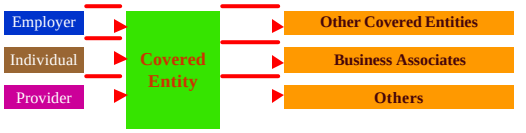
Scope of HIPAA

PRIVACY	TRANSACTIONS	SECURITY
•Disclosure •Use Restrictions •Consent/ Authorization •Audit Rights	•Format •Conditions •Content •Codes	•Physical •Electronic •Encryption •Assessment and Planning

Scope of HIPAA



The Six Things Covered Entities Should Worry About Under HIPAA



HIPAA Requirements

Notice
Permission
Access
Security
Responsibility
Oversight

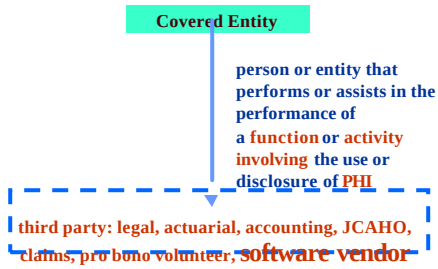
HIPAA Enforcement "For Dummies"

- Civil sanctions for violation of standards
- Except if you ***did not know***
- Exercising ***reasonable diligence*** you ***would not have known*** of violation
- Penalty waived if violation due to ***reasonable cause*** & ***not willful neglect***
- 30 days + to cure & technical advice
- $100 for each violation or $25,000/year

HIPAA For Crooks

- ***Unlawful use or disclosure***
- $50,000 + 1 year in jail
- $100,000 + 5 years for false pretences
- $250,000 + 10 years in jail if with ***intent*** to sell, transfer or use health information for commercial advantage, personal gain, or malicious harm

A Business Associate is?



It's What You Do: Disclosures that do not create a Business Associate

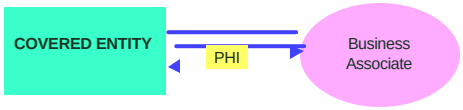
- To the individual
- To a provider for treatment
- To a member of the *workforce*
- To certain financial institutions with respect to certain payment matters
- To sponsor of Health Plan
- Among jointly administered government health programs
- To health oversight agency

Do Business Associates Worry About HIPAA?

If not itself a Covered Entity, a Business Associate is NOT directly regulated by HIPAA

BUT …….

Satisfactory Assurances



Before Using or Dislosing PHI:

Covered Entity must obtain in writing *satisfactory assurances* that the business associate will properly safeguard the information

Contractual Provisions

Three categories of provisions:

I. Permitted and required uses and disclosures

II. Specific covenants

III. Termination Provisions

I. Permitted and Required Uses and Disclosures by Business Associate

- **Generally state all permitted uses and disclosures**
- **May include management and administration of BA's business**
- **May include data aggregation services**

I. Special Issue: Data Aggregation

- PHI from different Covered Entities for comparative analysis
- Note: a Covered Entity could not do this directly without consent from each individual

I. Disclosures by Business Associate

A Business Associates may disclose PHI,

provided in each case that any disclosure by a BA either:

- **is required by law, or**
- **Authorized and BA obtains "reasonable assurances" that information will be held confidential and used only as required by law or for the purposes disclosed and**
- **disclosee notifies BA of any known breach**

II. 9 Specific Covenants

Business Associate will:

1. **Not use or disclose PHI inappropriately**
2. **Use appropriate safeguards**
3. **Report unauthorized use or disclosure**
4. **Supervise Agents**

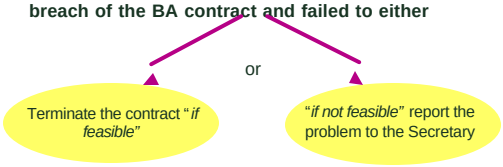
5 - 7. Enable access/amendment/audit

8. **Books and Records**
9. **Return or Destroy PHI**

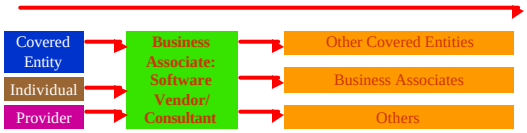
III. Termination

Covered Entity could be in violation of HIPAA:

If the Covered Entity knew of an uncured "pattern of activity or practice" by the Business Associate in breach of the BA contract and failed to either



The 3 HIPAA Concerns For Business Associates

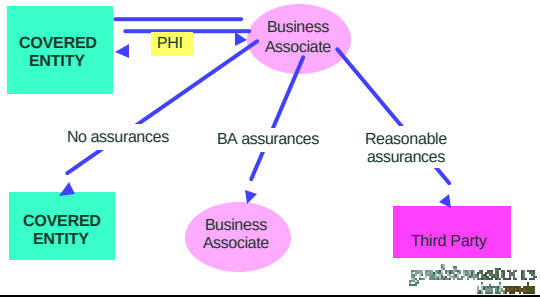


HIPAA Requirements → Written Contract, Permission, Assurances, Termination → Impact On Operations, Sufficient Scope, Achievable Performance, Risk Management

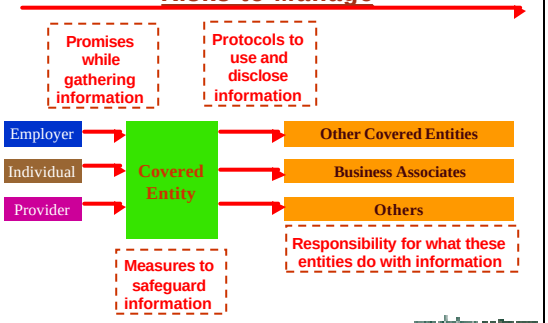
HIPAA and Risk Management

- **Our Premise:**
  The Management of the Risks Engendered by HIPAA Will Establish a Protocol That Can Be Applied in Managing Other Risks to the Enterprise, Whether Similar or Not, and Whether Clearly Understood at the Outset, or Not

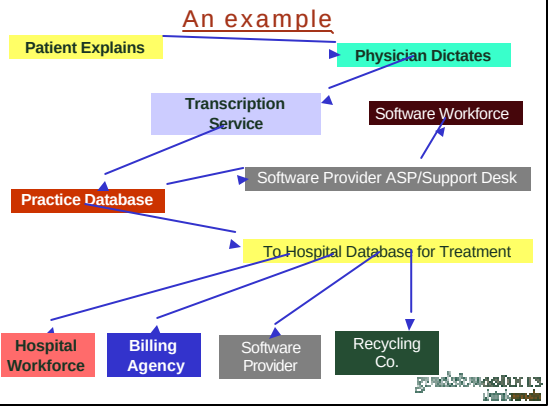
Managing Risk: Disclosures by a Business Associate



Organizations with Consumer Information Have Privacy and Security Risks to Manage



An example



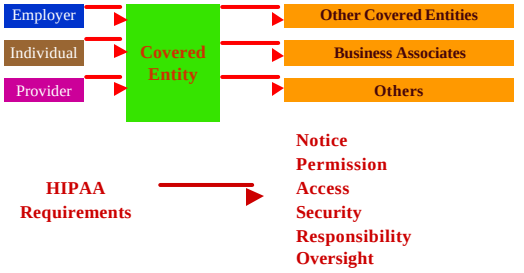
Managing the Risk

- Evaluation and Assessment of the Risk
- Establishment of Threshold Protocols
- Establishment of Regulatory Exemptions
  - Make the Risk Go Away
- Contract
  - Transfer the Risk by Agreement
- Insurance
  - Transfer the Risk for a Price
- Retention
  - Reserve for the Risk

Insurance as a Risk Management Tool

- What was Available
  - Liability Policies
    - CGL, Exclusion Buybacks, Extended Coverages
  - Errors and Omissions Policies
  - Directors and Officers Policies
  - Performance and Payment Bonds
  - Manuscript Policies
- Insurance specially for HIPAA
- September 11 and the insurance market

The Six Things Covered Entities Might do to use HIPAA to Manage Risks



HIPAA Requirements

Notice
Permission
Access
Security
Responsibility
Oversight

Summary

- HIPAA may be new, but privacy and security risks are not
- HIPAA itself is a guide for risk management

HIPAA Loss Prevention and Business Associates: A Risk Management Perspective

October 26, 2001

Alan M. Reisch
areisch@goulstonstors.com
Steven J. Snyder, Esq.
ssnyder@goulstonstorrs.com

goulston&storrs
thinkresults