Health Care Privacy – Insuring HIPAA Compliance Through Business Associate Contracts

Edward Janger
Brooklyn Law School

January 23, 2007

HIPAA's Regulation of Business Associates

- Covered entity must contract for data protection.
- The Business Associate's obligations are based in contract rather than HIPAA itself.
- Are there risks associated with contractual protection?

Risks of Contract Based Regulation

- Contract risk
  - Credit Risk
    - Bankruptcy – *Toysmart*
    - Insolvency
  - Other Externality Problems
    - *Card Systems*
    - Detection
    - Damages
    - Monopoly
- Lack of relationship with regulator
- Lack of relationship with customer
- Irreparability of harm

Credit Risk -- Bankruptcy

- Bankruptcy – *Toysmart*
  - If the business associate goes bankrupt, it may choose to breach its contract with the HIPAA entity and sell the data.
  - 2005 Amendments to the Bankruptcy Code include a response to Toysmart
    - The Leahy Amendment
      - Data cannot be sold in violation of a privacy policy unless
        - » Privacy ombudsman appointed
        - » Ombudsman negotiates for, and court approves sale with appropriate privacy protections.

Credit Risk – Limitations of the Leahy Amendment

- There must be a privacy policy.
  - The Leahy amendment only provides protection if the debtor has a privacy policy that limits disclosure.
  - In consumer contexts this is increasingly uncommon.
- Healthcare may be different.
  - In healthcare contexts, the Leahy amendment may provide meaningful protection where the covered entity has negotiated for appropriate contractual protections.
- The Leahy amendment only applies if the debtor files for bankruptcy.

Risk of Thinly Capitalized Business Associates

- Insolvency undercuts the incentive to take care.

General Risks of Contract Based Regulation

- Detection problems
  - Violation of contract may not be detected
  - Even if it is detected, the source of the data leak may not be ascertainable
- Damages problems
  - Individual harms are likely to be small
  - Damages are unlikely to cause internalization of cost.
- Monopoly problems
  - Card Systems may be the only game in town . . .

Attenuated relationship with consumers

- Entity with a B2C relationship does not necessarily suffer reputational harm when an Business Associate breaks its contract.

Attenuated relationship with regulator

- Regulated entity satisfies its obligation under HIPAA by entering into a contract with the Business Associate.
- Is the covered entity liable if the BA breaks its contract.