The Data Breach Nightmare – Minimizing the Litigation Exposure

Michael Vatis
Steptoe & Johnson, LLP
New York, NY
mvatis@steptoe.com
212-506-3927
“Litigation” Risks

- Civil lawsuits
  - Including class actions

- Agency enforcement actions
  - Health and Human Services (HHS)
  - Federal Trade Commission (FTC)
  - State regulators
Civil Lawsuits

- HIPAA provides no “private right of action”
  - i.e., does not allow for private citizen to bring lawsuit based on violation of the statute

- But Security and Privacy Rules can be cited as setting a “standard of care” that can be used in a lawsuit based on “negligence”
Civil Lawsuits

- Challenges for plaintiffs:
  - Showing concrete “injury in fact” to be able to sue in federal court (“standing”)
  - Showing that defendant was negligent
  - Proving that plaintiff suffered compensable harm

- Plaintiffs getting more inventive in proving they have standing to sue

- Run aground on showing harm
Agency Enforcement Actions

- For now, greater risk of enforcement action by agencies
- HHS
- FTC
- State Regulators
Wellpoint, Inc. – 2013

$1.7 million to settle action

Failed to secure e-PHI of applicants for insurance after software upgrade.
  – No policies/procedures to authorize access to database
  – No adequate technical evaluation
  – No safeguards to verify authorized users

Even though no evidence or fraud or identity theft
Idaho State University – 2013

$400,000 to settle, plus corrective action plan

For 10 months, disabled firewall, leaving e-PHI unsecured

For five years, failed to conduct risk analysis, inadequately implemented security measures, and no procedures to review system activity to determine if there was a breach
HHS

- Hospice of North Idaho -- 2013
- $50,000 settlement with small hospice
- Theft of laptop with e-PHI of 441 individuals
- Failure to conduct regular risk analysis, esp of portable devices
- Failure to implement appropriate security measures
HHS

- Massachusetts Eye and Ear Infirmary -- 2012
- $1.5 million settlement and corrective action plan
- Theft of unencrypted laptop with e-PHI of over 3,500 patients
- Inadequate risk analysis and policies to restrict access only to authorized users of portable devices
- No confirmation that data was ever accessed
HHS

- Blue Cross and Blue Shield of Tennessee -- 2012
- $1.5 million to settle, and corrective action plan
- Theft of 57 unencrypted computer hard drives from leased facility
- Contained recordings of customer service calls with PHI of 1 million individuals
- Inadequate physical access controls
HIPAA: Who’s covered?

- “Covered entities”
  - Health plans, health care clearinghouses, certain health care providers

- Business associates
  - Data processors, claims processors, billing firms, lawyers, accountants, consultants, benefits managers, etc.

- Subcontractors of business associates
State Regulators

- Massachusetts Attorney General
- Goldthwait Associates and pathology groups -- 2013
- $140,000 settlement by medical billing company that mishandled and inappropriately disposed of medical records
- Paper records in disposal facility
- Violation of state data security laws
- Physicians violated state laws and HIPAA by not hiring appropriate service provider and implementing safeguards to protect personal information given to the provider
State Regulators

- Massachusetts Attorney General
- South Shore Hospital -- 2012
- $750,000 settlement; requirement of third-party audit
- Violation of HIPAA and state data security law
  - Lost back-up computer tapes with personal information of hundreds of thousands of individuals
  - Information unencrypted
  - Never informed contractor that tapes contained personal and health information
  - Failed to determine whether contractor had sufficient safeguards
State Regulators

- Health Net of the Northeast -- 2010
- Lost portable computer with PHI of 1.5 million individuals, over a third Connecticut residents
- CT Attorney General--$250,000 payment to state (and $500,000 more if data misused)
- Violation of HIPAA and state breach notification law because of six month delay in notification
State Regulators

- Health Net of the Northeast (cont.)
- Second settlement with CT Insurance Department
- $375,000 settlement for violation of state laws requiring “good management” by insurers and conformity with federal and state confidentiality laws (and another $25,000 two years later)
- Failure to properly secure and protect personal information, and to timely notify department of the breach
- Must provide credit monitoring services and personal identity insurance
Breach Notification Laws

- Requirement to notify affected individuals and (sometimes) state regulators
- HIPAA
- 47 states plus D.C., Puerto Rico, Guam, US Virgin Islands
- Most state laws limited to SSN, financial information
- Some include health information
Data Breach Toolkit

- Privacy and Security Assessment
  - Network security
    - Access controls, authentication, firewalls, encryption, password policies, intrusion detection, log retention, etc.
  - Identify and map data
  - Policies and procedures
  - Contracts with business associates; subcontractors
  - Training
  - Privacy statements and actual practices
  - Cyber risk insurance
  - Test your Incident Response Plan
When the Breach Occurs

- Incident Response Plan
  - Mobilize necessary personnel
    • Legal
    • IT
    • Forensics
    • Communications
  - Containment and analysis
    • Stem the damage
    • Secure the network
    • Preserve evidence
    • Identify the source

- Notification
  - Determine scope of breach, affected information, affected individuals
  - Who must be notified?

- After-action review
  - Remediation
  - Improve response procedures
Questions?

Michael Vatis  
Steptoe & Johnson LLP  
mvatis@steptoe.com  
212-506-3927  
E-Commerce Law Week:  www.steptoe.com  
Weekly Podcasts:  www.steptoeCyberblog.com
The Data Breach Nightmare – Minimizing the Litigation Exposure

Kirk J. Nahra
Wiley Rein LLP
Washington, D.C.
202.719.7335
KNahra@wileyrein.com
@kirkjnahrawork

(April 22, 2014)
My Presentation

- Discuss litigation risks and best practices
- Focus on prevention and good security practices
- Address primary areas of concern
Overall Status on Litigation

- Volume of privacy-related litigation has been small, but steadily increasing
- Wide range of litigation related to security breaches and identity theft
- Courts have been skeptical of many claims
- Is a breakthrough case on the horizon?
- Is “negligence” a viable theory?
Why Hasn’t There Been More Litigation?

- Typically, there has been no private cause of action in most privacy statutes or regulations (e.g., HIPAA, GLB)
- Substantial difficulties with proof of damages (both as an incentive to bring cases and as an element of a claim that can survive a motion to dismiss)
- Limited government enforcement as a stepping stone to class litigation
Damages are a Real Hurdle

- Smith v. Chase Manhattan Bank
- Financial institution gave list to third party, received payments on sales
- Said it didn’t do these things in privacy notice
- No damages alleged/no cause of action
- Only unwanted telemarketing
Litigation Risk

- So, what drives litigation risk?
- Security Breaches (first, second and third on this list)
- Best practice is to be smart about data security and dealing with security breaches
- “Privacy” issues have not led to much litigation (although this can change)
Litigation Risk

• Be smart about protecting your data
• Focus on data that can lead to problems
• Act quickly and responsibly when there is a breach
• Mitigation
• Make sure your notices are responsible
Privacy and Litigation

• Marketing issues
• Data Ownership
• Data as an asset
• Privacy Notices – Misstatements
Litigation – Consumer Litigation

- Also recent litigation from patients seeking compensation when their de-identified data is being sold.
- An interesting development in trying to create patient-centered class actions
- Creates concerns both about how de-identified data can be used and about efforts from health care entities to profit from selling de-identified data
Litigation Impact

• Claims are unlikely to succeed (and cases have been dismissed for now), BUT they are focusing attention on how patient and health care data is being sold and disclosed

• This can affect both the HIPAA environment (where HHS is evaluating the de-identification rules) and the overall perceptions of the impact of healthcare data

• Watch these cases (and any new ones) carefully
The HIPAA Security Rule

- Detailed provisions
- Focus is on process and documentation
- This means (1) you can have good overall security without HIPAA compliance and/or (2) HIPAA Compliance without actual good security.
The Security Rule

- The biggest impact on business associates is the need to comply with the HIPAA Security Rule
- "Lift up" your security program from "reasonable and appropriate" to full compliance with the HIPAA Security Rule
- This affects actual practices and documentation
Key Remaining HIPAA Challenges

• **Breaches Generally**
• Way too many breaches continue to happen
• Make sure you are reviewing your overall security practices
• Pay close attention to problems faced by others
• Encrypt anywhere you can
Insider Access issues

• One key area of challenge for all health care companies – mis-use of access by employees
• This is a real and significant ongoing issue
• Close down access where you can
• But increase your controls where you can’t
Mitigation

- Identifying the problem
- Determining the cause of the problem
- Evaluating any potential harm from the problem
- Stopping the bleeding from the problem
- Evaluating appropriate changes (if any)
- Determining any other legally required steps (or appropriate business steps)
- Does mitigation require notification to individuals?
The FTC and Health Care

- The FTC actively pursues security cases
- FTC used general security enforcement approach, to go after what seems to be a HIPAA covered entity
- FTC also is filling in gaps from HIPAA
- Remember them as an additional enforcement agency
Security Conclusions

• Best defense is a good defense
• Realistic enforcement concerns, from a variety of directions
• Companies must constantly adjust to developments involving technology and developments involving other companies
• Requires a serious ongoing effort to stay at or ahead of the curve
• Act quickly and responsibly when there is a problem
Questions?

- Kirk J. Nahra, Wiley Rein LLP
- 202.719.7335
- knahra@wileyrein.com
- @kirkjnahrawork
- Subscribe (for free) to Privacy in Focus - http://www.wileyrein.com/publications.cfm?sp=newsletters.