"Security and Privacy After September 11: The Healthcare Example”

Professor Peter P. Swire
Ohio State University
Consultant, Morrison & Foerster LLP
April 25, 2002
Overview

- Introduction
- Security and Privacy after September 11
  - Can you report a terrorist/patient?
  - More emphasis on security
  - What implication for privacy?
- Proposed Rule Changes & Consumer Groups
  - Some surprises: FDA exception, employer exception, hybrid entity changes
I. Background

- Clinton Administration Chief Counselor for Privacy
- Unusual double major:
  - White House coordinator for HIPAA medical privacy rule, 1999-2000
  - Chair, White House task force on how to update wiretap and surveillance laws for the Internet age
Currently

- Ohio State University College of Law
  - Director D.C. program
- Consultant, Morrison & Foerster, with focus on medical privacy (materials available today)
- Full version of this talk forthcoming, Minnesota Law Review
- www.osu.edu/units/law/swire.htm
II. Reporting Suspicious Activity

- Rule issued before Sept. 11. How well does it work today?
- What if a suspected terrorist is in the hospital? Can you report that?
- Example: patient exposed to anthrax, and you suspect person involved in making or distributing spores
When Can You Report?

- National security exception
- Avert serious threats to health or public safety
- Law enforcement rules generally
National Security Exception

- Section 512(k)(2)
- May disclose PHI “to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities”
- Those activities as defined in law -- what you expect as “intelligence”
Averting Serious Threats

- Section 512(j) permits voluntary disclosure by a covered entity
- Must be “consistent with applicable law and standards of ethical conduct”
Averting Serious Threats

- Option 1, can disclose where:
  - “Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public”; and
  - “Is to a person or persons reasonably able to prevent or lessen the threat”
Averting Serious Threats

- Option 2, disclosure OK where:
  - “Is necessary for law enforcement authorities to identify or apprehend an individual”
  - “Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim”
  - That is, confessions to violent crimes
Averting Serious Threats

- Can’t disclose where confession is made as part of therapy for propensity to commit violent conduct
- Conclusion: the rule allows disclosure to avert serious threats, including by terrorists
Sec. 512(f) generally requires “in response to law enforcement official’s request”

Covered entity can’t volunteer the information, except where required by a reporting law or requested by law enforcement
General Law Enforcement

- Court order, grand jury subpoena, administrative subpoena for full file
- To locate or identify a suspect, fugitive, material witness, or missing person:
  - Name, SSN, limited other information
Summary on law enforcement

- For anthrax suspect:
  - Likely national security
  - May have evidence, in good faith, of imminent threat
  - Can respond to law enforcement requests more broadly

- The rule holds up better than you might have expected to this new challenge

- But, still limits on your disclosure to the police
Security & Privacy Today

- Greater focus on (cyber) security
- Security vs. privacy
- Security and privacy
Greater Focus on Security

- Less tolerance for hackers and other unauthorized use
- Cyber-security and the need to protect critical infrastructures
- Back-up needed in case of cyber-attack, attack on payments system, electricity grid, telephone system, or other systems you need
Security vs. Privacy

- Security sometimes means greater surveillance, information gathering, & information sharing
- Computer trespasser exception in USA Patriot Act
- Report possible terrorists
- Err on the side of public health reporting
- In short, greater disclosures to foster security
Security and Privacy

- Good data handling practices become more important -- good security protects PHI against unauthorized use
- Audit trails, accounting become more obviously desirable -- helps some HIPAA compliance
- Part of system upgrade for security will be system upgrade for other requirements, such as HIPAA privacy
Greater law enforcement & anti-terrorism urgency after September 11

Medical privacy rule already has provisions to respond to September 11:
- Public health
- Report terrorists

Not clear so far that need changes here to HIPAA privacy rule
III. Comments on the Rule

- Public debate to date about:
  - Consent vs. acknowledgment
  - “Marketing”

- Watch for these issues from consumer side:
  - New public health exception, especially for drug companies
  - New exception for employee records
  - New “hybrid entity” provision
Public health uses and disclosure

- From 12/2000 rule
  - PHI can be disclosed to a public health authority “authorized by law to collect or receive such information”
  - PHI can be disclosed where *required* by the FDA or under other applicable law
Public health changes

- Proposed rule would allow disclosure to:
  - Any person subject to FDA jurisdiction
  - “For the purpose of activities related to the quality, safety, or effectiveness” of an FDA regulated product or activity
  - No re-use limits on those who receive data
  - Major provision for the drug companies?
Employee Data

- New exclusion from definition of PHI for
  - “Employment records held by a covered entity in its role as employer.”
  - Limiting language in preamble.
  - But the regulatory text is very broad -- those records are entirely outside of the rule.
Hybrid entities

- Current law:
  - If “primarily” a covered entity, then all your operations are covered.

- Proposal:
  - Covered entity defines components that are covered

- Example:
  - If no standard transactions, could a hospital web site be outside the rule? Sell all data?
Concluding Thoughts on Security

- Biggest messages today:
- Data handling will have to improve
- Computer security will get more attention and budget
- Critical systems will need to be robust against new threats
- Better data handling, in general, will lead to better privacy compliance, too
How the Proposed Rule Looks to the Consumer Groups

- Consent -- Senator Kennedy hearings
- “Marketing” -- many activities now excluded from the definition
- FDA exception -- gift to drug companies
- Employee exception -- gift to employers
- Hybrid entities -- invitation to create loopholes and surprise consumers
Finally

- Industry will continue to identify issues where the rule is burdensome or HHS needs to provide clarification
- Consumer groups have their talking points, as well
- Look for continued fireworks
Contact Information

- Professor Peter Swire
- Phone: (301) 213-9587
- Email: swire.1@osu.edu
- Web: www.osu.edu/units/law/swire.htm
- Presidential Privacy Archives: www.privacy2000.org