"Security and Privacy After September 11: Implications for Healthcare"

Professor Peter P. Swire
George Washington Law School
Consultant, Morrison & Foerster

HIPAA Summit

October 25, 2001

Overview

- Introduction
- Health care after September 11:
  - Public health
  - Can you report a terrorist/patient?
- New anti-terrorism law & health care
- Security and Privacy after September 11
  - More emphasis on security
  - What implication for privacy?

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

- Visiting Professor, GW Law School
- Consultant, Morrison & Foerster, especially for medical privacy
- Current writings on the anti-terrorism law and computer security
- www.osu.edu/units/law/swire.htm

II. Public Health

- Sec. 512(b) fairly broad
- PHI can be disclosed to a public health authority “authorized by law to collect or receive such information”
- Permitted purposes include public health surveillance, investigations & interventions

Public health (cont.)

- Disclosure also permitted, if authorized by law, to a person exposed to or at risk for a disease
- *Uses* permitted by a covered entity that is a public health authority whenever it is permitted to disclose that PHI

Public Health -- Conclusions

- The rule permits what needs to be disclosed, if it is “authorized by law” -- check that
- Proper data handling needed by public health agencies:
  - Privacy -- good practices for patient data
  - Security -- make sure network is protected and data cannot be tampered with

III. 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

General Law Enforcement

- 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

IV. New Anti-Terrorism Law

- Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism
- USA PATRIOT Act
- Barney Frank . . .

Some Relevant Provisions

- In general, changes to wiretap laws, foreign intelligence, money laundering, new terrorism crimes, etc.
- Some health care issues:
  - Biological weapons
  - Grand jury secrecy changed
  - Nationwide search orders
  - Computer trespasser exception

Biological weapons statute

- Sec. 817
- 10 years jail for knowing possession of any "biological agent, toxin, or delivery system of a type or in a quantity, that, under the circumstances, is not reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose"

Grand Jury Secrecy Changed

- Current law: separation between law enforcement (grand jury, constitution applies) and foreign intelligence
- New law: “All the walls are down now” between FBI, CIA, etc.
- Example: you release PHI to grand jury, & records can go to foreign intelligence without notice to you or a judge

Nationwide search orders

- Current law: you must respond to an order from judge in your local federal district
- Section 220 USA-PATRIOT:
  - "Electronic" evidence: e-mail and web surfing records
  - Binding order from any federal judge in the country
  - What if the order seems overbroad? Must contest with that distant judge.

Computer Trespasser Exception

- Current law:
  - Under ECPA, can monitor your own system for security
  - Can turn over evidence of past hacker attacks
  - Can’t invite law enforcement to “surf over your shoulder” to investigate possible ongoing attacks -- that has been considered an open-ended wiretap

Computer Trespasser (cont.)

- Sec. 217 USA Patriot
- Now system owner can invite law enforcement to surf over the shoulder
- Only for
  - "Computer trespassers" with no reasonable expectation of privacy
  - Relevant to an investigation
  - No communications other than those to/from the trespasser

Computer Trespasser (cont.)

- Can covered entities authorize this surfing over the shoulder?
- Will PHI be disclosed? What if hacker downloads PHI?
- New & tricky issues under HIPAA
- Never any hearing on the provision -- may need guidance

V. 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 electricity grid, telephone system, or other systems you need

Security *vs.* Privacy

- Security sometimes means greater surveillance, information gathering, & information sharing
- Computer trespasser exception
- 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

Concluding Thoughts

- 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

Concluding Thoughts

- 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

Contact Information

- Professor Peter Swire
- Phone: (301) 213-9587
- Email: pswire@law.gwu.edu
- Web: www.osu.edu/units/law/swire.htm

- Presidential Privacy Archives: www.privacy2000.org