“HIPAA and the War on Terrorism”

Professor Peter P. Swire
Ohio State University
Consultant, Morrison & Foerster LLP

HIPAA Summit West
June 7, 2003
Overview

- Introduction
- HIPAA, National Security, and Domestic Security
  - “Retail”: The suspected anthrax terrorist
- Security and Privacy in the War on Terrorism
- Public Health & Bioterrorism
  - “Wholesale”: Surveillance of populations
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; other computer security work
Currently

- Ohio State University College of Law
  - Director D.C. program
- Consultant, Morrison & Foerster, with focus on medical and other privacy issues
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
- Public health exception (later)
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, under standard statutory definition of “intelligence”
National Security Exception

- How it looked in 2000
  - “Retail” -- individual requests for records when needed for a specific intelligence investigation
  - The anthrax incident, and likely permitted to disclose if the suspected terrorist is in the ER
National Security Exception

■ How it looks today
  - “Wholesale” -- Total Information Awareness and proposals to create huge intelligence databases, including many health records
  - TIA de-funded domestically by Congress
  - It may continue, and ongoing proposals to create bioterrorism databases

■ Covered entities “may” disclose but are not required to disclose under HIPAA
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

- 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 Anthrax Suspect

- 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 the post-9/11 world

- But, still limits on your permitted disclosure to the authorities
III. Security & Privacy In the War on Terrorism

- Greater focus on physical and cyber security
- Security vs. privacy
- Security and privacy
- More on this in the law review article, in materials or at www.peterswire.net
Greater Focus on Security

- Less tolerance for hackers and other unauthorized use
- Physical and Cyber security and the need to protect critical infrastructures
- Back-up needed in case of cyber-attack, such as 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
- TIA, Bioterrorism Centers, Patriot Act
- Report possible terrorists
- Err on the side of public health reporting
- In short, greater disclosures to foster security
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 should be system upgrade for other requirements, such as HIPAA privacy.**
One privacy innovation

- E-Government Act of 2000
- Requires a “privacy impact assessment” for new federal computer systems
- OMB guidance to be issued shortly
- Note: the statute authorizes the PIA to be kept secret in cases of national security
IV. Public Health Uses and Disclosures

- The basic rule under Sec. 512(b):
  - PHI can be disclosed to a public health authority “authorized by law to collect or receive such information”
  - This includes “public health surveillance, public health investigations, and public health interventions”

- Sec. 512(a) -- can also disclose where “required by law”
Once PHI goes to an “authorized public health agency”, no further use or disclosure limits.

Consistent with HIPAA, public health agency can disclose to:

- Bioterrorism Centers
- DOD and Total Information Awareness
- Research
- Private marketing uses, etc.
Why this “Loophole”?

- Federalism -- HHS shouldn’t control state public health agencies
- Those agencies usually not covered entities
- Too darn complicated to extend business associate contracts to all those agencies with their multiple missions
- Not thinking about “Total Information Awareness” in 1999 and 2000
Bioterrorism Initiatives

- Jan. 2002, $1.1 billion in block grants for bioterrorism preparedness
- To receive, states must submit a “comprehensive plan” to HHS for public health and preparing for a bioterror attack
- June 2002 additional $$ for vaccines and communications systems
- Perhaps total of $3 billion so far
Bioterrorism and the Model Act

- CDC supports Model State Emergency Health Powers Act
- Rushed to completion after 9/11
- HHS pressure to adopt the Act as condition of receiving funding
- Almost have the states have adopted it
The Model Act

- Broad emergency powers
- Must report “all cases” that “may be potential causes of a public health emergency”
- Must report “unusual” prescription rates, types of prescriptions, or trends in pharmacy visits that “may be …”
- Is this reporting “required by law”?  
  - Likely yes
Critiques of Model Act

- “Emergency” powers too broad
- Almost no privacy or data security provisions
  - Disclosure to any person having a “legitimate need”
- The Model Act for public health systems and privacy has not gone forward
Going Forward on Public Health

- As state agencies get a once-in-a-generation infusion of bioterrorism funds, they should build in privacy and security at the same time.
- Federal funds should require compliance with privacy and security, not push the Model Act in ways that lack those.
- Otherwise, we may see these as feeder systems for TIA.
Public Health and HIPAA

- Potential for public health exception and bioterrorism initiatives to create feeder systems for TIA
- Undo much of what HIPAA tries to accomplish
  - Lack of transparency in what data is being shared with whom
  - HIV history and role of confidentiality in getting treatment and stopping public health emergency
  - Health professionals as spies for the government?
Concluding Thoughts

- Overall, HIPAA was built with national security and domestic security in mind.
- The change now is TIA and related data mining initiatives.
- We need broader public debate on how to reconcile the public safety and privacy goals.
Concluding Thoughts

- These issues will continue for a long time
  - As long as terrorism is a major threat
- As keepers of medical records, you are usually permitted to disclose under HIPAA but generally not required to disclose
- You can enter the public debate in your state about how to fight terrorism and also keep surveillance within bounds
- Good luck in this effort
Contact Information

- Professor Peter Swire
- Phone: (240) 994-4142
- Email: peter@peterswire.net
- Web: www.peterswire.net