“Privacy and Security: Lessons from Non-Health Sectors”

Professor Peter P. Swire
Moritz College of Law
The Ohio State University

HIT Symposium at MIT

July 17, 2006

Overview

- My background
- Importance of privacy & security to deployment of health IT
- Two key issues, informed by non-health experiences:
  - Preemption
  - Enforcement
- Explain the consumer, industry, & political perspectives on these issues
- Conclusion: the choice we face

Swire Background

- Now law professor, based in D.C.
  - Active in many privacy & security activities
- Chief Counselor for Privacy, 1999-2001
  - U.S. Office of Management & Budget
  - WH coordinator, HIPAA privacy rule
  - Financial, Internet, government agency privacy
  - National security & FISA
  - Computer security

Background

- Health care since 2001:
  - Written on health privacy & security topics, at www.peterswire.net
  - Consulted on HIPAA implementation
  - Markle, Connecting for Health
  - Deidentification – Tuesday talk here
- Next Monday, free conference at Center for American Progress on “The Internet and the Future of Consumer Protection”, at www.americanprogress.org

Privacy, Security & the NHIN

- As public policy matter, crucial to get the benefits of data flows (electronic health records) while minimizing the risks (privacy and security)
- As political matter, privacy and security are the greatest obstacles to adoption
  - Focus group – the emergency room while out of town as the *only* scenario that got substantial majority to favor EHRs
  - Many individuals see risks > rewards of EHRs

Implications of Public Concern

- All those who support EHRs must have good answers to the privacy and security questions that will be posed at every step
- “Trust us” not likely to be a winning strategy
  - The need for demonstrable, effective protections
  - The system must be strong enough to survive the inevitable data breaches & resultant bad publicity

Preemption

- Industry perspective:
  - Benefits of data sharing high – “paper kills”
  - Shift to electronic clinical records is inevitable; that shift has occurred in other sectors
  - Can only run a national system if have a national set of rules
  - Preemption is essential – a “no brainer”

Preemption: Consumer View

- Janlori Goldman, Health Privacy Project
- A *lot* of state privacy laws
  - HIV
  - Other STDs
  - Mental health (beyond psychotherapy notes)
  - Substance abuse & alcohol
  - Reproductive & contraceptive care (where states vary widely in policy)
  - Public health & other state agencies
- HIPAA simply doesn't have provisions for these topics – if preempt, then *big* drop in privacy protection

Consumers & Preemption

- Link of reporting and privacy
  - HIV and other public health reporting *based* on privacy promises
  - So, objections if do reporting w/out privacy
- Concrete problems of multi-state?
  - Many RHIOs have only one or a few states
  - Build out from there
  - State laws both as “burdens” (industry) and “protections” (consumers)

Preemption & Politics

- Consumer and privacy advocates see states as the engine for innovation
- Current example: data breach
  - California went first, and now Congress is trying to catch up with a uniform standard
- Basic political dynamic – industry gets preemption in exchange for raising standards nationally

Preemption in Other Sectors

- Gramm-Leach-Bliley: no preemption
  - But, Fair Credit 2003 does some of that
- Wiretap (ECPA): no preemption
- Data breach: proposed preemption
- FTC unfair/deceptive enforcement: no preemption
- CAN-SPAM: significant preemption
- Conclusion -- variation

Key Issues in Preemption

- Scope of preemption matters & can vary
- One policy baseline: scope of preemption matches the scope of the federal regime
  - If the scope is for networked health IT, then preemption about that, not entire health system
- Preserve state tort and contract law?
- Preserve state unfair & deceptive enforcement?
- Grandfather existing state laws? Some of them?

Summary on Preemption

- Strong pressures for preemption in national, networked system
- If simply preempt and apply HIPAA, then have a dramatic reduction in privacy & security
- This is a major & complicated policy challenge that is not likely to have a simple outcome

Enforcement

- The current “no enforcement” system
- Key question for the NHIN:
  - Can the current no-enforcement system be a credible basis for EHRs and the NHIN?

The No Enforcement System

- Imagine some other area of law that you care about – violations are serious.
- Batting average: 0 enforcement actions for 20,000 complaints
- Enforcement policy: one free violation
- Criminal enforcement:
  - DOJ cut back scope of criminal penalties
  - *No* prosecution for the > 200 criminal referrals
  - 2 cases brought by local federal prosecutors

Effects of No Enforcement

- Signals work
  - Surveys already showing lower efforts at HIPAA compliance and lower reported actual compliance by covered entities
  - Contrast internal HIPAA efforts and budget (low enforcement) with compliance efforts on Medicare fraud & abuse (hi enforcement)
- Why should Congress and consumer groups trust compliance with HIPAA, much less with new rules for the NHIN?

Other Privacy Enforcement

- Fair Credit, stored communications, video rentals, cable TV
  - Federal plus private right of action
- Deceptive practices, CAN-SPAM, COPPA, proposed data breach
  - Federal, plus state AG
- HIPAA as outlier, with federal-only enforcement
  - If feds don't do it, then have no enforcement of the HIPAA rules themselves

What We Have Learned

- Within health IT debates, consensus statements often sound like this:
  - Need preemption to do the national network
  - Should not punish/enforce against covered entities, when they are struggling in good faith to implement new HIPAA mandates
  - Of course, privacy and security should be part of the NHIN, but likely don't go beyond HIPAA requirements

What We Have Learned

- That trio of conclusions, based on experience in other sectors, may face serious political obstacles:
  - Preemption is likely to be partial and require new federal standards in some areas
  - The “no-enforcement system” will be hard to sustain
  - New privacy/security protections quite likely will accompany new NHIN data flows

Conclusion: Your Choice

- Option 1: Play Hardball
  - Decide the costs of privacy & security are too high to be built into the NHIN
  - Push a strategy of high preemption and low enforcement
  - Grudgingly give only the bare minimum on privacy/security when the political system forces it onto industry

The Better Choice

- Option 2: A NHIN to Be Proud Of
  - Incorporate the key values of state laws – especially for sensitive data – into the NHIN
  - Support reasonable enforcement, so that bad actors are deterred and good actors within covered entities get support
  - Build privacy & security into the fabric of new systems, not just as a patch later
    - Connecting for Health as an example

The Better Choice

- With the second option – A NHIN to Be Proud Of – the patients are not treated as the political enemies
  - The risk of political backlash is less
  - The quality of the NHIN for actual patients is higher
- That, I think, should be our goal
- Thank you

Contact Information

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