The Future of Privacy and Security

Regulatory, Business, and Health IT Perspectives

STANLEY NACHIMSON

NACHIMSON ADVISORS, LLC

DECEMBER 14, 2007

THE FIFTEENTH NATIONAL HIPAA SUMMIT

Privacy and Security

- Timely topic as we expand the electronic interchange of health information.
- Gets lots of interest from press, government oversight agencies, interest groups.
- I believe that there is a lack of knowledge and misunderstanding about the true nature of these topics and the public interest.

Privacy vs. Security

- These are two very different concepts (at least, according to me).
- Privacy
  - Policy oriented
  - Personal choice
  - Can be generally understood by the public
  - Slow changing once set
  - Determined by government, public policy, interest groups, etc.
  - Need relatively uniform policies and practices throughout the country to support interoperability

Privacy vs. Security

- Now, let's contrast that with Security
  - Technical! – for IT types
  - Falls on entities to develop and implement
  - Rapid changes in threats and technologies
  - Hard for public to understand details
  - Need to be able to interoperate, but can be different from entity to entity.
  - Requires an investment by entity, but hard to see ROI

Focus on Privacy

- HIPAA brought issue to the forefront in the health industry.
- Truth is, privacy has been an issue since information has existed!
- Today, we are dealing with the increase interchange of information for many purposes in health care:
  - Administrative
  - Treatment
  - Public Health
  - Marketing

Focus on Privacy

- Has been a national focus on health care privacy
  - Congress has hearings
  - ONC criticized for not developing a privacy framework
  - Interest groups decry the lack of privacy protections
  - HITSP working on privacy constructs
- There is a perceived need to protect individuals' information.
- New definition of privacy proposed by Donald Kerr, a deputy director of national intelligence.
  - Privacy can no longer mean anonymity. It should mean that government and businesses properly safeguard people's private communications and financial information.

We Like to Share

- Yet, there is an individual propensity to not keeping things private.
- Many examples of known and unknown information sharing by individuals
  - Supermarket and other retailer frequent shopper cards
  - Web site registrations
  - Internet generation much more willing to share
    - Recent USA Today article indicated that those who use Facebook or Myspace are more willing to put information out there so that they can connect with peers.
    - Some folks don't realize the extent of their sharing – recent principal caught with some embarrassing pictures and comments on her Myspace page.

Risk vs. Reward

- Privacy decisions are truly risk vs. reward decisions, both for individuals and for the public good.
- Some of the rewards of sharing information –
  - Better care thru coordination and understanding of an individual's condition.
  - Improved public health with the identification of trends
  - Better research
  - More targeted and effective marketing
  - Better information for public planning of services to individuals

Risk vs. Reward

- But what are the risks of sharing that information?
  - Discrimination
  - Legal and illegal threats
  - Public/private ridicule
  - Unfair conclusions about an individual

So What Will the Future Be Like?

- Difficult balance for policymakers will continue, keeping controversies alive.
- But progress is necessary for acceptance of new HIEs. Patients need to understand privacy so they will participate.
- Need more openness and choice in privacy rules
- Individual authorizations are difficult to manage.
- Each person needs to be able to set their own rules.
- Entities must make the rules more clear. Need to move away from considering privacy just a matter of signing some papers.

Security

- A very different environment from privacy
- Security is a technology issue
- And security is a business issue
  - There are costs
  - There are risks
  - Need to strike a balance
- Purpose of security - to get right information about the right person to the right person at the right time.
  - Availability, integrity, confidentiality

Security

- But the problem -
- Rapidly changing environment
  - Changes in health care IT technology
    - Needed remote computing guidance as this was not even envisioned in the original CMS security rule.
    - Today we have iPods, PDAs, Blackberries, iPhones, and who knows what is next (recent CSI on WiFi body suit).
    - We don't know all of the security threats involved with these
    - New techniques coming to production – e.g. biometrics
  - Changes in threats to entities
    - New viruses, worms, etc. keep coming in. Attempts become more and more difficult to control.
    - Now we have Mac viruses and worms.
    - Easy to fool even sophisticated users.
    - Some users (especially at home) don't even bother with protections.
    - Inside threats!

Current Regulatory Status

- Difficult for regulators
- Need to recognize the genius, and the foolishness, of the HIPAA Security Rule
  - Genius to set guidelines and let each entity design their security controls based on their own needs
  - Foolish to think that entities could do it without more specific guidance.
  - Entities looked at this as a one time job, not a continuing process.

How to Handle This

- Security is something best left to the technicians, the vendors.
- Rapidly changing
- Tough to regulate and enforce
- Businesses need to make decisions on risk and investment
- Large businesses are recognizing importance
  - IBM commits to spending $1.5 billion to improve security
  - Purchases of smaller vendors to enhance security offerrings

Future Regulatory Efforts

- CMS moving toward proactive reviews?
  - Some work with OIG
  - Will do some more detailed audits on entities complained against
  - Will help encourage entities to protect security
- Specific standards will be difficult to produce
- CCHIT certification criteria developed for security aspects of EHRs.

Need to Develop the Business Case

- We must provide education on security.
- Need to explain the risks and rewards.
  - What are the significant risks?
    - Regulatory penalties?
    - Threats from hackers?
- There is a cost, but what does it buy?
  - Is peace of mind enough?

The Big Question

- Do We Really Care About Privacy and Security in Health Care?
  - Government does
  - Interest groups do
- But does the person on the street (in general) care?
- Maybe not until their information is misused – and then maybe not eve then.

Evidence to the Contrary

- Look at breaches to date
  - Banks have lost some tapes
  - Federal agencies have had laptops stolen
  - TJX had major breach of data
- What was the reaction
  - Some temporary righteous indignation that it happens
  - A little bad press
  - But it seems to pass
  - Credit monitoring is offered
  - Has anyone gone out of business?

Evidence to the Contrary

- HIPAA Privacy and Security was considered a burden
  - In fact, many folks considered it an invasion of their privacy!
- The average person seems to trust that their information will be safe, or simply doesn't care or understand.

The Bigger Question

Should we care?

The Bigger Answer

- Of Course
- It's never a problem unless it happens to you!
  - Impact on individual
  - Impact on entity
- Need to assure that privacy and security are built into our systems, not an add on
- Need to consider how we stop the bad things from happening when we build our HIEs
- Need to provide education to the public about why the protection is needed.

My Contact Information

- Nachimson Advisors, LLC
- Nachimson_advisors@verizon.net
- 410-935-7084