

HIPAA Privacy and Beyond: Fundamentals and Key Challenges

Kirk J. Nahra
Wiley Rein & Fielding LLP
Washington, D.C.
202.719.7335
KNahra@WRF.com

March 7, 2004

Wiley Rein & Fielding LLP



Key Issues

- HIPAA Highlights
- For covered entities, employers and business associates
- Understand where it applies and where it does not
- HIPAA Security Primer
- Other issues to watch out for in the health care industry
- What does the future hold?



State of the HIPAA Rules

- Privacy
 - Final Final – Published August 14, 2002
 - Compliance date – April 14, 2003
 - “Small” health plans – April 14, 2004
- Standard Transactions
 - Real Compliance date – October 16, 2003
 - Implementation of Contingency Plans
 - Substantial confusion/Ongoing problems
 - Concern about the “train wreck”
- Security
 - Compliance date is April, 2005
 - Don’t ignore security component of privacy



Health Care Privacy: How We Got Here

HIPAA Statute/1996

Administrative simplification and privacy
(intersection of business developments and law)

- Congress missed August 21, 1999 deadline
- Responsibility fell to HHS

Final Rule - published December 28, 2000 (Clinton)

Final Final Rule -- August 14, 2002 (Bush)

Compliance date -- April 14, 2003



Privacy Rule

- Effective April 14, 2003
- No widespread problems
- Ongoing efforts to comply
- Systemic problems based on unexpected/unconsidered variations
- Inconsistent compliance
- Lots of conservatism



Enforcement to Date

- No “public” enforcement
- Lots of complaints
- HHS still struggling with challenges
- Complaints have focused on a couple of key areas:
 - Privacy notices/lots of confusion (mainly providers)
 - Mistakes
 - Treatment problems
 - Spouses, family members (covered entities not disclosing enough)



Privacy Problems - Example

- Houston hospital
- Internal Employee
- Sold Patient Records about accident cases to plaintiff's lawyers
- High visibility problem
- Potential criminal sanctions



More problems - Subcontractors

- California hospital hired transcription company in Texas, subcontracted to another company in Florida, eventually subcontracted to an individual in Pakistan
- Threatened to release PHI on the Web
- Lots of concerns, increased issues with BAs and subcontracting
- May be a lingering focal point



Who Must Comply with HIPAA?

- Health plans (health insurers)
- Health care providers
- Health care clearinghouses
- Employers? Not directly – big issue
- Other insurance entities (e.g., life, auto, disability)? No
- Business associates (indirectly)



Key Concepts

- TPO- Treatment, Payment and Health Care Operations
- PHI- Protected Health Information
- Business Associate
- Minimum necessary
- Covered entity



Rules of Disclosure

- PHI may not be used or disclosed by covered entities except as authorized by the individual who is the subject of the information or as explicitly provided by the rules.
- Exchange of protected health information should be relatively easy for core health care purposes – TPO - and more difficult for purposes other than health care.



Key Risk Areas

- Employment
- Marketing
- Spouses
- Individual rights
- Broadly applicable issues
(code word – class action)



HIPAA and Employers

- Very complicated
- At least confusing/perhaps inconsistent
- Opportunities and challenges
 - Shift to fully insured?
 - Will customers abandon group health care?
 - Keep an eye on this



Employer/Group Issues

- Rules make little sense
- Mass confusion
- Likelihood of mistakes
- Customer relations
- Will require significant changes



What Is The Issue?

Avoid having PHI used by employers for employment-related purposes

- HHS' fix:
 - HHS does not directly regulate employers or other plan sponsors
 - Instead, HHS places restrictions on the flow of information from covered entities to non-covered entities, including plan sponsors



Issues for Employers

- PHI touch points
- Employee service
- Making practical sense of the regulation
- Vendor contractors (brokers, consultants, disease management)
- Policies and procedures
- Good practices



HIPAA Privacy and Security

Each [Covered Entity] who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical and physical safeguards:

- (A) To ensure the integrity and confidentiality of the information;
- (B) To protect against any reasonably anticipated threats or hazards to the security or integrity of the information; and unauthorized uses or disclosures of the information; and
- (C) Otherwise to ensure compliance with this part by the officers and employees of such [covered entity].

42 USC 1320d-2(d)(2)



HIPAA Statute

Requires HHS Secretary to prepare rule addressing:

- (i) The technical capabilities of record systems used to maintain health information;
- (ii) The costs of security measures;
- (iii) The need for training persons who have access to health information;
- (iv) The value of audit trails in computerized record systems; and
- (v) The needs and capabilities of small health care providers and rural health care providers.



Privacy Rule

- Covered entity “must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.”
- Any “business associate” under the Privacy Rule must agree by contract to “use appropriate safeguards to prevent use or disclosure of [PHI] other than as provided for by” the business associate contract.



HIPAA Security Rule

- Ensure integrity, confidentiality and availability of electronic protected health information
- Protect against reasonably anticipated threats or hazards, and improper use or disclosure
- Ensure compliance by workforce



Security Standards General Concepts

- Flexible, scalable
 - Permits standards to be interpreted and implemented appropriately from the smallest provider to the largest plan
- Comprehensive
 - Cover all aspects of security-behavioral as well as technical
- Technology neutral
 - Can utilize future technology advances in this fast-changing field



- Appropriate measures based on:
 - The size, complexity, and capabilities of the covered entity;
 - The covered entity’s technical infrastructure, hardware, and software security capabilities
 - The costs of particular security measures; and
 - The probability and criticality of potential risks to electronic protected health information
 - A covered entity under the Rule may use “any security measure that allow the covered entity to reasonably and appropriately implement the standards and specifications” of the Security Rule



Steps

- Most of the Security Rule describes an appropriate “process” that covered entities must go through in evaluating security options, broken down into technical, physical and administrative safeguards
- “Risk analysis” means to:
 - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity
- “Risk management” involves an obligation to:
 - Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [the Security Rule.]



Administrative Safeguards

- Sanction policy
- Assigned responsibility for security activities
- Security awareness and training
- Contingency planning
- “Security incident” procedures (a “security incident” is an “attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system”)



Physical Safeguards

- Facility access controls (limiting physical access to information systems)
- Workstation use policies
- Workstation security, and
- Device and media controls (such as procedures for disposal of computer hardware in light of recent reports of privacy violations involving discarded computers that still retained PHI)



Technical Safeguards

- Access controls (such as unique user identification automatic log-off and emergency access procedures)
- Audit controls integrity (protection against improper alteration or destruction of PHI)
- Person/entity authentication and transmission security



New Security Issues

- Higher awareness of security concerns
- More visible problems
- New contract requirements for business associates
- Link to security developments in other areas
- May lead to more questions about BA relationships



TriWest Case

- Data contained on network servers stolen
- Links to other areas (military information, terrorism)
- Aggressive precautions on identity theft/notification/PR
- New procedures for all military contractors
- Follow-up litigation (562,000 members)
- Lawsuit dismissed – no actual damage



Litigation

- History to date
 - Much less than anticipated
- Why not?
- Little Enforcement
- Key Issues
 - What is the claim?
 - Who is it by?
 - What are the damages?



Smith v. Chase Manhattan Bank

- Financial institution gave list to third party, received payments on sales
- Said it didn't do these things in privacy notice
- No damages alleged/no cause of action
- Only unwanted telemarketing



Recent California Privacy-Related Legislation – The Major Activity

- Cal. 168 – SSN Numbers
- SB 1 – Financial Information/G-L-B
- Information Security – Notification of Security Breaches
- Other Key Laws to Worry about and watch – 15 new privacy laws passed in 2003



Key California Issues

- Geographic scope
- Private cause of action
- Enforcement
- Feasibility



Key ramifications

- Direct exposure?
- Effect on the federal debate
- Spotlight on certain practices
- Influence around the country
- Setting standards in undefined areas



SSN Legislation – What does it say?

- SB 168 prohibits a “person or entity” from
 - publicly posting or displaying an individual’s SSN,
 - printing an individual’s SSN on any card required for the individual to access products or services.
 - requiring an individual to transmit his/her SSN over the Internet (unless encrypted),
 - requiring an individual to use his/her SSN to access the Internet web site, or
 - printing an individual’s SSN on any materials to be mailed to the individual unless (a) required by law or (b) used in connection with applications and forms sent by mail.



What it Doesn't Do

- Does not prohibit:
 - using SSN completely
 - mailing information to a third party (such as a medical provider, broker, TPA, or employer) that contains an individual's SSN or
 - using SSNs in the internal administration of the various products and services
 - mailing materials that include SSNs if such materials constitute “applications” or “forms”



Geographic Scope

- No discussion of geographic scope in the statute itself.
- The measure reasonably applies to all entities using the SSN of a California resident
- SB 168 does not include any language that would limit its reach to only companies based or licensed in California



More geographic scope

- Direct application of the statute's prohibitions to “any person or entity” strongly suggests the statute is intended to apply to any entity using the SSN of California residents
- The enforcement process for “out-of-state” entities is not clear, but best guess is that the words of the statute apply to California residents, and therefore the safest course of action is to comply for all California residents.



What has happened elsewhere?

- SSN Legislation in at least six other States
- Arizona (mainly ID cards, some grandfathering), Connecticut (same), Georgia (ID cards), Missouri (public display and posting), Texas (like California, some grandfathering), Utah (ID cards).
- Proposed in at least 12 other states
- More to come in 2004 – is there any doubt?



SB 1 Terms – Financial Privacy

- SB 1 requires a financial institution to obtain the “explicit prior consent” of a consumer before it may share nonpublic personal information with any nonaffiliated third party (opt in).
- No prohibition on “offering incentives or discounts to solicit a specific response to the notice”



More SB 1 Terms

- The consumer must be provided with the opportunity to direct that personal information not be disclosed to joint marketing partners (opt out).
- Where nonpublic personal information is shared with affiliates outside of the statutory exceptions, a financial institution must notify the consumer and provide the consumer a right to opt out of these disclosures.



Even More SB 1

- SB 1 provides for unrestricted sharing of information between a financial institution and its wholly-owned financial subsidiaries in the same line of business (e.g., insurance or banking) where the subsidiaries operate under a common brand.
- SB 1 provides an exception (with certain restrictions) that allows a financial institution to market its own products and services, or the products or services of another entity, to customers of the financial institution, without an opt in or an opt out.



Key Questions

- Geographic Scope - California consumers
- Enforcement civil penalties, \$2500 per violation, A.G. or functional regulator can bring action
- No Private Cause of Action
- Effective Date – July 1, 2004
- Federal Changes – What's left?



Security breaches

- Notice must be given to any data subjects who are California residents in the event of an unauthorized acquisition of (unencrypted) computerized data that compromises the security, confidentiality or integrity of personal information – data was or is reasonably believed to have been acquired by unauthorized person – effective July 1, 2003.
- Name plus (1) SSN, (2) Drivers license or Cal. ID # or (3) financial account or credit/debit card number.



Notice

- In the most expedient time possible and without unreasonable delay
- Caveats for legitimate needs of law enforcement or necessary measures to determine scope of breach and restore integrity to system
- Notice in writing or electronic (if allowed by E-SIGN)



Best practices - OPP

- Collect minimum amount of personal information necessary (and retain for minimum time necessary)
- Inventory records systems, critical computing systems and storage media to identify those containing personal information.
- Classify personal info. according to sensitivity



More Best Practices

- Use appropriate physical and technological security safeguards (paper as well as electronic)
- Promote awareness of security and privacy
- Require third party service providers to follow your security policies and procedures – and monitor and enforce
- Use intrusion detection technology



More Best Practices

- Use data encryption wherever feasible
- Dispose of information in a secure manner
- Review security plan at least annually



What will happen?

- How will this play out in California?
- Effects on development of nationwide security practices – e.g., TriWest case and testimony in support of Feinstein legislation
- Effects on HIPAA practices/Enforcement
- California best practices as national practices
- Third party issues – enormous risks



What else is happening

- SB 27 (Figueroa) Consumer rights for personal information held by non-financial institutions.
- AB 715 (Chang) Restrictions on disclosure of PHI for marketing (some exceptions, but cause of action and punitives)
- AB 763 (Liu) Prohibits visible mailing of SSNs (where mailing of SSN is allowed)



More

- AB 68 (Simitian) Online privacy. Web sites must have a privacy policy and must comply with it.
- SB 186 (Murray) Spam legislation. Prohibits sending of spam to or from a California e-mail address without direct consent.



What's Next

- Legislation to ban medical data from going to contractors abroad? (State Senator Figueroa) - Resulting from disclosure of PHI to Pakistani Transcriber



Getting Started on HIPAA

- Audit of information use/practices
- Work HIPAA into contract negotiations/
renegotiations
- Educate employees
- Educate business associates
- Educate providers



Conclusions

- Very difficult balancing act
- Ongoing confusion
- Keep an eye on the lawsuits/enforcement
- Be conscious of where people can complain – and where they may not
- Expect continued conservatism
- Follow “other” medical privacy laws
- An ongoing issue that will not be going away



The Future

- Watch for continuing problems
- Small likelihood of legislative change (no one is sure what to do)
- Some possibility of “other” medical privacy legislation (e.g., FCRA)
- Still a high profile issue
- Watch for “visible” problems

