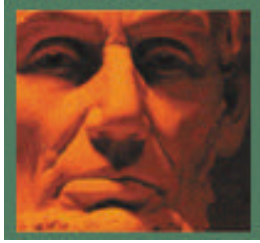
Third National HIPAA Summit
Privacy Officers Association Preconference
October 24, 2001

Wiley Rein & Fielding LLP



# *Contemplating, Committing to, and Conquering Privacy Compliance Challenges*


***William A. McGrath***
***wmcgrath@wrf.com***
***202.719.3146***

# *Approach*

- Privacy in an Overall Context
- Accepting the Intensified “Privacy” Environment
- Major Privacy Provisions
- Implementation Considerations

# *Privacy In An Overall Context*

- Where Have We Been?
- Where Are We Now?
- Where Are We Going?

# *Privacy In An Overall Context*

- Where Have We Been?
  - Confidentiality vs. Privacy
    - Traditional view -- doctor-patient confidentiality
    - Tech revolution has increased vulnerabilities
    - Patient and public concerns
    - Increase in governmental oversight

# *Privacy In An Overall Context*

- Where Have We Been?
  - Traditional Theories of "Privacy" Protection
    - 4th Amend, U.S. Constitution
    - Privacy Act of 1974
    - Fair Credit Reporting Act
    - ADA and FMLA
    - State Constitutions
    - State Statutes
    - Common Law Invasion of Privacy

# *Privacy In An Overall Context*

- Where Are We Now?
  - From Confidentiality to Privacy
    - More comprehensive than simply avoiding inadvertent or inappropriate disclosures
    - Policies and systems to govern collection, use and maintenance of information
    - Education and notice
    - Access to and right to amend records about yourself
    - Accountability

# *Privacy In An Overall Context*

- Where Are We Now?
  - HIPAA
    - Statute passed in 1996; Title II, Administrative Simplification; Congress missed 8/20/99 deadline; HHS responded
    - Standards for the Privacy of IIHI (the “Privacy Rule”)
      - Intersection of business developments and law
      - December 28, 2000 Final Rule Issued; April 14, 2001 Effective Date; April 14, 2003 Compliance Date; Guidance Issued July 6, 2001

# *Privacy In An Overall Context*

- Where Are We Now?
  - HIPAA
    - Standards for  Electronic Transactions
      - August 16, 2000 Final Rule Issued; October 17, 2000 Effective Date; October 17, 2002 Compliance Date
    - Security Standards
      - August 12, 1998 Proposed Rule Issued

# *Privacy In An Overall Context*

- Where Are We Now?
  - Gramm-Leach-Bliley Act ("GLBA")
    - Notice, if required, by July 1, 2001
    - Administrative Policies and Procedures – PR Pending
  - State Statutes
    - 21 States enacted Privacy Laws in last year
    - Continued Aggressive Action
  - Regulatory Uncertainties

# *Privacy In An Overall Context*

- Where Are We Going?
  - Privacy in the context of national concerns: impact of September 11th attack
  - An evolving landscape
    - HIPAA Guidance; anticipated modifications
    - HIPAA current constitutional challenges
    - GLBA – continued concern regarding notices; implementation of policies and procedures; pending legislation

# *Privacy In An Overall Context*

- Where Are We Going?
  - Have we gone too far?
  - Have we not gone far enough?
  - Are we where we should be?

# Have We Gone Too Far?

# *Have We Gone Too Far?*

- *E-Health Law & Policy Report*

  Strict Privacy Bill Fails in California (Oct.1, 2001)

- New York Times

  A Nation Challenged: Plan to List Who Receives Disaster Aid Stirs Concern (Sept. 27, 2001)

# *Have We Not Gone Far Enough?*

- New York Times
  A Cautionary Tale for a New Age of Surveillance (Oct. 7,2001)

- Los Angeles Times
  AOL Using Bugs, Cookies, to Help Target Ads (Oct. 8, 2001)

- Federal Trade Commission
  FTC Chairman Announces Aggressive, Pro-Consumer Privacy Agenda

# *Are We Where We Should Be?*

- ***Congress of the United States***

  ***House of Representatives, Committee on Ways and Means***
  Implement HIPAA Administrative Simplification Without Delay (Oct. 3, 2001)

- BNA Health Care Daily

  National Governor's Association Wants Delay in Implementation of HIPAA Standards for Electronic Transactions

# *Accepting the Intensified Privacy Environment*

- Stages of Acceptance
  - How to prepare your organization
    - Doing what is right
    - Maintaining competitive posture
    - Establish a new marketing tool
    - Develop your privacy philosophy.
  - How to prepare your customers and business associates
    - Education and training
    - Who is drafting your business associate agreements?
    - Implementation

# *Major Privacy Provisions*

- HIPAA
- Gramm-Leach-Bliley
- State Statutes

# *HIPAA*

- HIPAA – Some Issues to Highlight
  - Individually Identifiable Health Information
  - Covered Entities
  - Business Associate
  - Consent vs. Authorization
  - Is HIPAA Subject to Change?
  - Is HIPAA at Risk?

# *What is Protected Health Information?*

- oral or recorded information relating to past, present or future physical or mental health of an individual or provision or payment of health care
- that is individually identifiable -- reasonably can be used to identify the individual to which it pertains
- created or received by a covered entity

# *HIPAA*

- Individually Identifiable Health Information ("IIHI")
  - Protected Health Information
  - Summary Health Information
  - De-Identified Information

# *HIPAA*

## Who is a covered entity?

- health plans
- health care clearing houses
- health care providers who electronically transmit health information in connection with standard transactions
  - an HCP is a person who furnishes, bills or is paid for health care in the normal course of business
  - health care encompasses care, services or supplies related to the health of an individual

# HIPAA

- Covered Entities – *Group Health Plans*
  - Definition of GHP – employer sponsored welfare benefit plans are covered if they have 50 or more participants or are administered by an entity other than the employer
    - Thus under definition, if GHP has <50 participants and is administered by an entity other than that employer = covered GHP
    - Only GHP not covered = <50 participants and self-administered by employer

# *What are rules for use and disclosure of PHI?*

- rules do not mandate disclosure, except to individual and HHS
- minimum necessary standard
  - not applicable to requests by HCP for treatment purposes
  - burden on requestor to comply
- notice, consent and authorization

# HIPAA

- Business Associates
  - Requirements for Business Associate Agreement
    - Establish permitted and required uses and disclosures of PHI
    - Require reporting to covered entity uses and disclosures of PHI not permitted by contract
    - Include flow-down restrictions in contracts with agents and subcontractors
    - Permit individuals right of access, accounting, and amendment

# HIPAA

- Business Associates
  - Contracting Considerations
    - Covered Entity
      - Whether the Business Associate Agreement ensures that the business associate is financially liable for all violations of the Privacy Rule by the business associate, or its agents or subcontractors?
      - Whether the Agreement requires the business associate to assume the cost of becoming and remaining HIPAA compliant?

# HIPAA

- Business Associates
  - Contracting Considerations
    - Covered Entity
      - » Whether there are issues beyond the minimum requirements for the Agreement that the covered entity believes should be included in the Agreement (*e.g.*, functions, activities, or services to be provided the business associate?
      - » Should the Agreement impose specific terms for implementing the minimum HIPAA Privacy Rule requirements?

# HIPAA

- Business Associates
  - Contracting Considerations
    - Does the covered entity seek to impose penalties on you as a business associate (*e.g.*, through an indemnification clause)?
    - If penalties are imposed, do they relate only to your minimum HIPAA business associate obligations, or do the penalties have broader application?
    - Are your HIPAA Privacy Rule obligations limited only to the PHI created, received, used, or disclosed, or do Privacy Rule obligations attach to non-covered products (*e.g.*, workers' compensation)?

# HIPAA

- Business Associates
  - Contracting Considerations
    - Does the Business Associate Agreement contain terms beyond those minimally required by the HIPAA Privacy Rule?
    - If so, are these terms linked to the business associate requirements?
    - Does the Agreement address the cost of *becoming* HIPAA compliant (*e.g.*, amending relevant contracts with agents and subcontractors), particularly if you also are not a covered entity in your own right?

# HIPAA

- Business Associates
  - Contracting Considerations
    - Does the Agreement address the cost of *remaining* HIPAA compliant (*e.g.*, costs of producing an accounting)?
    - Does the Business Associate Agreement seek to implement the requirements in ways that you believe are not warranted?
    - If so (and even if not), do you want to qualify any of the minimum requirements?

# HIPAA

- Consent vs. Authorization
  - Consent
    - Mandatory for direct treatment providers
    - Optional for health plans
    - Reasons health plans might want consent:
      - Custom or habit
      - Litigation avoidance
      - Client request
  - Authorization
    - Mandatory if use PHI outside the scope of TPO, national priority purposes, and other limited exceptions

# *Is HIPAA Subject to Change?*

- Sure – HHS Guidance
  - Rule by Reason
    - Mostly reassurance for HCPs.
    - "Substantial discretion" in implementing minimum necessary standard.
    - No soundproofing required, no need to provide logs of oral communications.
    - No expansion of current limits on marketing.
    - No expansion of Government access to PHI.
  - Rule Changes, Q&A guidance to come

# *IS HIPAA AT RISK?*

- Two pending court challenges
  - South Carolina
    - Unconstitutional delegation of legislative authority to HHS.
    - Beyond scope of authority delegated by HIPAA.
  - Texas
    - Beyond scope of authority
    - Violates Fourth Amendment, First Amendment, Tenth Amendment, Paperwork Reduction Act, Regulatory Flexibility Act.
  - Will they delay the clock? Not expected to right now, but stay tuned.

# *Gramm-Leach-Bliley Act "GLBA"*

- Applicable to Financial Institutions
  - Must be *significantly engaged* in financial activities described in section 4(k) of the Bank Holding Company Act to be considered a financial institution.
    - Credit counseling service
    - Medical service provider that establishes long term payment plans involving interest for significant numbers of customers
  - "Significantly Engaged" is a flexible standard

# *Gramm-Leach-Bliley Act "GLBA"*

- Obligations to both Consumers and Customers
  - Consumers – obtained a product or service
    - Initial notice of availability of privacy policy
    - Provide "opt-out" notice prior to sharing non-public personal information, with reasonable opportunity to opt out.
    - Advise of revisions to privacy policy and opt-out notice

# *Gramm-Leach-Bliley Act "GLBA"*

- Obligations to both Consumers and Customers
  - Customers –establishment of relationship
    - Initial privacy notice when relationship established.
    - Provide "opt-out" notice prior to sharing non-public personal information with non-affiliated third parties.
    - Annual Privacy Notice
    - Advise of revisions to privacy policy and opt-out notice

# *Gramm-Leach-Bliley Act "GLBA"*

- Current Environment
  - July 1, 2001 Deadline – has passed
  - No lawsuits filed yet
  - A great deal of publicity – ALL NEGATIVE
  - Nader *et al* petition regarding notices
  - FTC – considering revising notice requirements

# *Gramm-Leach-Bliley Act "GLBA"*

- Future Issues
  - Legislation introduced to revise GLBA
    - The Markey-Barton Bill
    - The Sessions-Pryce Bill

# State Law Issues

- HIPAA
  - No preemption of “more stringent” state laws
  - Patch-work of varied requirements
    - Laws addressing “sensitive” conditions
    - Authorization requirements
    - State Insurance Information and Privacy Protection Acts
  - Very aggressive landscape

# State Law Issues

- GLBA
  - GLBA does not preempt state laws that are not "inconsistent."
  - Laws that provide greater protection are not "inconsistent."
  - Activities by state Departments of Insurance
    - North Dakota, Connecticut, Illinois

# State Law Issues

- State Legislative Initiatives
  - Hawaii (HBs 1579 and 1604)
  - Illinois (HB 491)
  - Iowa (HB 110)

  If State Law Is More Strict, It Rules

  Beware of

  Coverage of Broader Class of Entities

  More restrictive marketing provisions

  Differing Time Frames for Implementation

# IMPLEMENTATION CONSIDERATIONS

- What is your privacy philosophy?
- Consider all applicable laws, including “more stringent” state laws.
- Work privacy requirements into contract negotiations and renegotiations now.
- Educate employees.
- Educate business associates.
- Educate customers.
- Stay tuned – Keep abreast of continued flux of federal and state statutory and regulatory environment.