HIPAA Compliance for Payor Organizations

Key Issues For Health Plans Under HIPAA Privacy Regulations

HCAA 2002 Annual Compliance Institute

April 21, 2002

Wendy L. Krasner
McDermott, Will & Emery
Washington, DC
wkrasner@mwe.com

Michelle M. Huntley
UnitedHealth Group
Minnetonka, MN
michelle_m_huntley@uhc.com
KEY ISSUES FOR HEALTH PLANS UNDER HIPAA PRIVACY REGULATIONS

I. Introduction
II. Implementation of Business Associate Requirements
III. Internal and External Disease Management Activities
IV. Affiliated Covered Entities/Organized Health Care Arrangements
V. Preemption -- State Privacy Requirements
I. INTRODUCTION

IMPORTANT CONCEPTS

- Insured vs. self-funded plans
- HMOs and insurers acting in their “issuer” capacity are referred to as “Health insurance issuers”
- Subsidiaries or affiliates acting in an “Administrative Services Only” capacity
- Health plan vs. employer sponsor of health plan
DEFINITION OF HEALTH PLANS

• An individual or group health plan that provides or pays for the cost of medical care is a “Covered Entity”
• It does not include any policy, plan or program providing or paying for the costs of “excepted benefits” -- e.g., disability coverage, automobile liability coverage, workers compensation or similar insurance
• “Group health plan” includes both insured and self-insured health plans, but there is an exception for group health plans with less than 50 participants that are self-administered
EMPLOYER SPONSORS AND BUSINESS ASSOCIATES

• Employer sponsors are not “Covered Entities” although Protected Health Information (PHI) provided to employer sponsors by group health plans subjects the employer sponsor to certain requirements depending on the nature and extent of the data

• An HMO or health insurer acting in an ASO role to a group health plan would be required to enter into a contract that complies with the business associate requirements to the extent they receive or use PHI in this capacity

• Neither the provision of insurance or HMO coverage by the health insurer requires a business associate contract

• In the M+C program, both CMS and the issuer are covered entities but not business associates
SUMMARY CLAIMS DISCLOSURES TO PLAN SPONSORS

• The group health plan, insurance issuer or HMO may disclose “summary health information” to the plan sponsor for either of the following reasons:
  – Obtaining premium bids from health plans for providing health insurance coverage
  – Modifying, amending or terminating the group health plan

• These activities combined with the plan sponsor’s conduct of the basic enrollment functions are not considered to be “plan administration functions”

• By restricting the kinds of information the plan sponsor receives, the plan sponsor can limit its obligations under the rules
DISCLOSURE FOR PLAN ADMINISTRATION FUNCTIONS

• Group health plans (and their health insurance issuers) may disclose PHI to a plan sponsor to carry out “plan administration functions” only in accordance with the requirements of § 164.504(f)(2)

• Plan documents have to be amended to incorporate certain required provisions (e.g., permitted uses and disclosures)

• The group health plan can disclose PHI to the plan sponsor upon receipt of a certification that the plan documents have been amended to incorporate the required provisions
DISCLOSURE FOR PLAN ADMINISTRATION FUNCTIONS

• The plan sponsor cannot use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.

• There has to be a “adequate separation” between the group health plan and the plan sponsor including provisions in the plan documents that describe the employees of the plan sponsor who have access to PHI and restrict such access to and use by such employees.
DETERMINATION OF MINIMUM NECESSARY

- Use or disclosure of PHI limited to Minimum Necessary with certain exceptions for disclosures
  - to or requests by health care provider for treatment
  - to the individual
  - requested by the individual
  - required for compliance with HIPAA standardized transactions
  - otherwise required by other laws

- “Reasonableness” standard
HEALTH CARE OPERATIONS

- Although consents are required of health care providers for the use or disclosure of PHI for purposes of treatment, payment or health care operations, they are not required of health plans.
- Key definition is “health care operations” in health plan context.
- Examples include: reviewing the competence or qualifications of professionals, business planning and development, premium rating and other activities related to the creation, renewal or replacement of a contract of health insurance.
- Definition is broad enough to include medical management and disease management activities.
REQUIRED AUTHORIZATIONS

- Authorizations are required for purposes other than treatment, payment, or health care operations.
- Health plans cannot condition enrollment or treatment on the individual’s providing such an authorization except under the following circumstances:
  - The authorization sought is for the health plan’s eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations prior to the individual’s enrollment in the health plan.
  - A health plan may condition payment of a claim for specified benefits on provision of an authorization if the disclosure is necessary to determine payment of such claim.
  - There are exceptions to both of the above when the use or disclosure of psychotherapy notes is at issue.
MARKETING AND HEALTH PLANS

- Marketing does not include communications that describe entities participating in health plan network
- Marketing does not include communications that describe the services or benefits covered under a plan of benefits
USE AND DISCLOSURE OF PHI FOR MARKETING

• PHI can be disclosed or used without an authorization for the marketing of health related products and services if the communication to an individual meets the following:
  – It must identify the health plan in making the communication
  – If the health plan has received or will receive direct or indirect remuneration for making the communication, then this fact is stated
  – It must contain instructions on how the individual may opt out of receiving future such communications
  – The communication must also explain why the individual has been targeted and how the product or service relates to the health of the individual
  – Consider the application of the above in the context of health plan pharmacy rebate programs
NOTICE OF PRIVACY PRACTICES

- Individuals have a right to adequate notice of the uses and disclosures of PHI.
- Where the individual is enrolled in a group health plan through an insurance contract or HMO, then the health issuer must give the notice.
- Where the health plan is self-insured, then the notice comes from the group health plan.
- Where the group health plan receives PHI from a health insurance issuer in addition to summary health information or information concerning the individuals’ enrollment, then maintenance and provision of notice by the group health plan is required.
- Notice can be provided to the named insured on the policy (e.g., to the subscriber as opposed to the subscriber and each of his or her enrolled dependents).
PRACTICAL APPROACH

• Covered Entity Status
  – Simple or complex operations

• Perform analysis of key provisions vs. current business practices
  – Methodology or tool must fit your business structure
  – Understand the flow of PHI internally and externally

• Establish Company position for key provisions
  – Minimum Necessary
  – Personal Representatives, Authorization and Consent
  – Business Associates
  – Disclosures of PHI, etc.

• Internal and External Communication Strategy
PRACTICAL APPROACH

• Develop specific action steps with accountabilities and dates
  – Electronic and Paper PHI
  – Consumer rights processes
  – Don’t forget websites, portals and other systems

• Project management and implementation

• Drafting the privacy notice

• Determining approach to training that is comprehensive
  – Classroom
  – Web-based
  – Additional training for specific high risk areas
II. IMPLEMENTATION OF BUSINESS ASSOCIATE REQUIREMENTS

DEFINITION OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (IIHI)

- Information that is a subset of health information, including demographic information collected from the individual, which:
  - Identifies the individual or
  - As to which there is a reasonable basis to believe that the individual can be identified

- “De-identified” information may not be useful
BUSINESS ASSOCIATE DEFINITION
TWO CATEGORIES

• If specific requirements are met, PHI may be disclosed to and used by Business Associates

• A person who performs or assists in the performance of a function or activity on behalf of the covered entity and which involves the use or disclosure of PHI

• Includes, but is not limited to:
  – Claims processing or administration
  – Data analysis, processing or administration
  – Utilization review
  – Quality assurance
  – Billing and repricing
  – Practice management
BUSINESS ASSOCIATE DEFINITION
TWO CATEGORIES

• Business Associates also include:
  – A person who provides any of the following services to or for a covered entity if the service involves the disclosure of PHI from the covered entity or another Business Associate:
    • Legal
    • Actuarial
    • Accounting
    • Consulting
    • Data aggregation
    • Management
    • Administrative
    • Accreditation
    • Financial
EXCEPTIONS TO BUSINESS ASSOCIATE DEFINITION

- Members of the covered entity’s workforce
- Entities that are merely conduits for information (U.S. Post office or the electronic equivalent)
- Financial institutions that process consumer payments for health care (assuming the covered entity complies with the minimum necessary requirements)
- Limited exception for entities that perform services as part of an Organized Health Care Arrangement
“SATISFACTORY ASSURANCE” REQUIREMENT

- A covered entity may disclose PHI to a Business Associate and allow the Business Associate to create or receive PHI on its behalf **only if** it obtains “satisfactory assurance” that the Business Associate will appropriately safeguard the PHI.

- “Satisfactory assurance” requires a written contract with specific provisions.
EXCEPTIONS FROM BUSINESS ASSOCIATE CONTRACT REQUIREMENTS

• Exceptions for disclosures
  – By a group health plan, health insurer, or HMO to the plan sponsor (if separate rules for plans are satisfied)
  – By a health plan that is a government program providing public benefits if an individual's eligibility or enrollment is determined by another entity, the activity is authorized by law and other requirements are met
LIABILITY OF COVERED ENTITY

• Brother’s Keeper Rule: A covered entity is not in compliance with the Privacy Regulations:
  – If the covered entity knew of a pattern of activity or practice of the Business Associate that constituted a material breach of the Business Associate contract
  – Unless the covered entity took reasonable steps to cure the breach or terminated the agreement or
  – If not feasible to terminate, report the violation to HHS

• Knowledge may arise from “substantial and credible evidence”
BUSINESS ASSOCIATE CONTRACT REQUIREMENTS

• The Business Associate must:
  – Not use or further disclose the PHI other than as permitted or required by law
  – Use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by the contract
  – Report any use or disclosure of the PHI not provided for by the contract of which it becomes aware
  – Ensure that agents and subcontracts agree to the same provisions
BUSINESS ASSOCIATE CONTRACT REQUIREMENTS

• The Business Associate must:
  – Make PHI available to the individual who is the subject of the health information
  – Make PHI available for, and incorporate any, amendments as required
  – Provide an accounting of disclosures upon an individual’s request
  – Make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary
BUSINESS ASSOCIATE CONTRACT REQUIREMENTS

• Termination provisions:
  – Must authorize termination by the covered entity if the covered entity determines the Business Associate has violated a material term
  – At termination of the contract, if feasible, all PHI received from the covered entity must be returned or destroyed. If not feasible, must extend protection of the contract to the information and limit further uses and disclosures to those purposes that make return or destruction infeasible
PRACTICAL ISSUES

• Business Associates are not directly subject to the Privacy Regulations (unless they are also a covered entity)
• What are the “appropriate safeguards” to prevent unauthorized use or disclosure?
• Business Associate not required to appoint a privacy officer or adopt specific policies and procedures
IMPLEMENTATION

• Develop template language
  – Distribute to all contracting parties for inclusion in new contracts

• Inventory all current contracts
  – Hold discussions with all business areas
    • What does the business associate do for you?
    • How is PHI used by the business associate?
    • How is PHI retained?
    • Any disclosures by the business associate?
  – Develop mechanism to track contracts and monitor inclusion of language

• Amend or Re-contract with business associate language
IMPLEMENTATION

• Business associate or not?
  – Firm identifies high risk patients for additional care
  – Company requests PHI in order to create national database of statistical information
  – Lab vendor requests PHI to do analysis of current lab costs, so that they can develop proposal to enter into new lab contract

• Disclose the minimum amount of PHI necessary to business associates
  – Have a methodology for review
    • Review electronic file record layouts
    • Identify non-electronic PHI
      – Remember External and Internal Audits, NCQA, etc.
IMPLEMENTATION

• Educate the business associate
  – Improper disclosures and appropriate safeguards
  – Final disposition of PHI by the business associate

• Enforcement
  – A violation becomes known - now what?
    • XYZ Company sends diabetes information to individuals on behalf of covered entity
    • “Trades” information to a retail pharmacy company
    • Retail pharmacy sends coupons for syringes, glucose tablets and other products to individuals
  – What actions if XYZ Company is an affiliated entity?
III. INTERNAL AND EXTERNAL DISEASE MANAGEMENT ACTIVITIES

DEFINITION OF DISEASE MANAGEMENT

- Definition of disease management was deleted from the final Privacy rule
- “Treatment” includes management of an individual’s health care by a provider
- Population based analyses to develop treatment protocols are health care operations (not treatment)
- Disease management companies may be providers or may be Business Associates of providers and/or plans
DISEASE MANAGEMENT ACTIVITIES

INTERNAL HEALTH PLAN ACTIVITIES

• If disease management (DM) falls within the definition of payment or operations, health plan may use and disclose PHI without individual consent or authorization

• Given broad definitions, this probably covers most DM activities

• Health plan needs policies and procedures to assure minimum necessary

• If health plan requires PHI from providers beyond what they would disclose for payment purposes, then provider agreements should require providers
  – To obtain patient consent for disclosure
  – To disclose the necessary PHI for DM purposes
DISEASE MANAGEMENT ACTIVITIES

EXTERNAL ACTIVITIES

• If outside organization assists in performance of DM must have Business Associate contract
• If health plan performs DM for self-insured group health plan, it must act as plan’s Business Associate
DISEASE MANAGEMENT ACTIVITIES

INDIVIDUAL RESTRICTIONS

• Individuals may request that providers and/or health plans limit use or disclosure of PHI
• Providers and plans not required to agree to requested limitations
• If they do agree, it may affect health plan’s DM activities
USE OF BUSINESS ASSOCIATES FOR QUALITY ASSURANCE ACTIVITIES

• Use and disclosure of PHI for quality assurance (QA) activities:
  – Authorized by the patient's consent as part of health care operations
  – Often performed by third party Business Associates
  – QA studies may be research (requiring an authorization) if the primary purpose is to produce “generalizable knowledge”
  – Avoid problems by clarifying scope of use in Business Associate agreement
EXAMPLES OF DISEASE MANAGEMENT ACTIVITIES

• Covered entity provides diabetes educational materials to their member population, using a printing and mailing vendor

• Pharmaceutical Company wants to provide “free” pamphlets and information to sick populations on behalf of the covered entity
  – Does this fall under the definition of disease management?
  – If so, do you have an appropriate agreement in place?

• Coordinating care through a nurse line
  – Internal operation or business associate
  – Personal representatives
IV. AFFILIATED COVERED ENTITIES (ACE) AND ORGANIZED HEALTH CARE ARRANGEMENTS (OHCA)

DEFINITION OF AFFILIATED COVERED ENTITIES

- Legally distinct covered entities that share common ownership or control may designate selves, or their health care components, as a single covered entity
- Common control exists if entity has power to significantly influence or direct actions or policies of another entity
- Common ownership exists if entity owns 5% or more of another entity
AFFILIATED COVERED ENTITIES (ACE)

- ACE treated as single covered entity
  - Must issue single privacy notice
  - Must appoint a single privacy official

- Advantages
  - Avoids Business Associate agreements between affiliates

- Disadvantages
  - Development of single privacy notice and uniform policies for companies that may be subject to disparate state privacy requirements not preempted by the Privacy Rule

- Examples
  - Multiple health plans under a common parent or holding company
  - Covered entities and non-covered entities under common ownership
ORGANIZED HEALTH CARE ARRANGEMENTS (OHCA)

- New term added in final HIPAA rule
- OHCA clinically integrated health care in which more than one covered entity participates, and covered entities
  - Hold selves out in public as participating in joint venture
  - Participate in joint activities including at least one of
    - utilization review
    - quality assessment and improvement
    - payment activities involving shared financial risk
- IPAs typical example of OHCA
  - IPA formed by large number of physicians
  - Common enterprise even if not under common ownership/control
  - May not practice in integrated clinical setting or share financial risk
  - If jointly engage in one or more of listed activities, will need to share PHI to undertake activity
ORGANIZED HEALTH CARE ARRANGEMENTS (OHCA)

THREE TYPES OF GROUP HEALTH PLANS:

• A group health plan and health insurance issuer or HMO but only with respect to PHI created or received that related to individuals who are or have been in the group health plan

• A group health plan and one or more other group health plans maintained by some plan sponsor (with same PHI limitation)

• A combination of group health plans maintained by same plan sponsor and health insurance issuer and HMOs with respect to such plans (with same PHI limitation)
V. PREEMPTION -- STATE PRIVACY REQUIREMENTS

PREEMPTIVE FRAMEWORK

• General rule
  A standard, requirement, or implementation specification adopted under HIPAA that is contrary to a provision of state law preempts the provision of state law

• HIPAA not a uniform privacy law
  – HIPAA controls in certain circumstances
  – State law controls in others
WHAT IS CONTRARY?

• A state law is “contrary” if
  “(1) A covered entity would find it *impossible* to comply with both the state and federal requirements;

  or (2) The provision of state law stands as an *obstacle* to the accomplishment and execution of the full purposes and objectives of [HIPAA].”

See 42 C.F.R. § 160.202
HOW HIPAA PREEMPTION WORKS

• Is it *impossible* to comply with both laws?
• To be impossible to comply with both laws,
  – HIPAA *prohibits* disclosure and state law *requires* disclosure

  OR

  – HIPAA *requires* disclosure and state law *prohibits* disclosure
HOW HIPAA PREEMPTION WORKS

Even if it is not impossible to comply with both laws, does the state law stand as an obstacle to accomplish the purpose of HIPAA?

A state law permits a health care provider to disclose information to a third party but HIPAA prohibits disclosure to the third party. It is not impossible to comply with both laws (state merely permits disclosure, does not require disclosure). But, if you comply with the state law, it would undercut HIPAA’s privacy requirements.
THE STATE LAW IS “CONTRARY.”
DOES AN EXCEPTION APPLY?

- State law more protective of privacy
- Examples
  - A state law imposes greater restrictions on a third party’s access to the information
  - Additional requirements on the form or substance of consent or authorizations
  - Additional law provides greater access to patient
- State laws provide greater access to patient
  - Greater rights to amend information, or receive more information about the types of uses or disclosures that a health care provider can make
THE STATE LAW IS “CONTRARY.”
DOES AN EXCEPTION APPLY?

- Any state law regarding disclosures to parents/guardians of minors
- Public health reporting
  - Reporting of diseases, injury, child abuse, birth, death, or reporting in connection with “public health surveillance investigation or intervention.”
- Secretary determination
  - See 42 C.F.R. § 160.203
PREEMPTIVE EFFECT OF HIPAA

Privacy practices that may need to change

- State law prohibits disclosure (HIPAA requires disclosure)
  - HIPAA requires disclosure in only two circumstances: (1) a request by an individual (except for certain psychotherapy notes); and (2) when required by the Secretary to investigate a health care provider’s compliance with HIPAA
  - There is no state law that prohibits an individual’s access to his/her protected health information
  - Any law that would prohibit disclosure to the Secretary without patient consent is preempted
MANAGING MULTIPLE STATES’ LAWS

Identification and analysis of state privacy laws

• Your own process
• Local industry groups
• Law Firms for analysis and specific questions
• HIAA Subscription Service
  – 50 State Analysis, including DC, Virgin Islands, Guam, Puerto Rico
  – state laws and regulations that directly regulate health plans, on-line and mail order pharmacies, utilization review organizations and TPAs
  – Medicaid managed care plans
  – AG opinions and case law
• AAHP considering a searchable database service that includes GLB, DOL, NCQA
• Consider multiple resources
MANAGING MULTIPLE STATES’ LAWS

• Example: Texas SB 11 Privacy Rules
  – Accelerated compliance date relative to HIPAA Privacy
  – Enumerates exceptions under which a covered entity must obtain authorization prior to disclosing PHI
  – Adjusts consent rules around re-identification of data
  – Provides different definition than HIPAA of marketing and related disclosure rules

• Operational Issues
  – Establishing policies, processes and systems logic to accommodate multiple states’ laws
  – Floor, ceiling or somewhere in the middle ground?

• State Enforcement and Violations