HIPAA Administrative Simplification for Employers

Presented at the 2003 HCCA Compliance Institute Conference
April 27-30, 2003

Mark E. Lutes, Esquire
Partner
Epstein Becker & Green, P.C.
1227 25th Street, N.W.
Suite 700
Washington, D.C. 20037
(202) 861-1824
mlutes@ebglaw.com
Presentation Goals

• What is HIPAA Administrative Simplification?
  – Background and Goals
  – Who is a Covered Entity?
  – Compliance Dates

• How do the Privacy Standards apply to employers and their sponsored health benefit plans?

• How do the Transaction Standards apply to employers and their sponsored health benefit plans?
Health Insurance Portability and Accountability Act (‘“HIPAA”) Background

• 1996 federal law addressing, *inter alia*, portability of insurance coverage, medical savings accounts, expansion of health care fraud and abuse laws

• Also established regulatory mandate for the creation and use of standards in the health care industry:
  – electronic transmission of transactions
  – privacy (i.e., use and disclosure) of individually identifiable health care information
  – security (i.e., maintenance and transmission) of individually identifiable health information
HIPAA - Applicability and Compliance Dates

• **Applicability:**
  - Health care providers who perform one of the enumerated transactions electronically
  - **Health plans**
  - Health care clearinghouses - “translators”
  - Business Associates - applicability limited to contractual requirements

• **Compliance Dates:**
  - Transaction Standards - October 2002, unless applied for an extension to October 2003
  - Privacy Standards - April 2003 (“small health plans” - under $5 million in premiums (insured) or claims (self-insured) - have until April 2004)
  - Security - To be determined
HIPAA - What is a “Health Plan”

An individual or group plan that provides, or pays the cost of, medical care, including, *inter alia*, the following:

- a group health plan other than one which self-administered and has less than 50 participants;
- a health insurance issuer;
- a health maintenance organization;
- Medicare and Medicaid programs; and
- any other individual or group plan or combination of individual or group plans that provides or pays for the cost of medical care.

**Employer’s ERISA plans and MEWAs are likely Covered Entities**
HIPAA - What is a “Health Plan”

Included:
- Health
- Dental
- Vision
- Health Reimbursement Accounts
- Prescription / MHSA carve outs
- Some EAPs

Excluded:
- Workers compensation
- Disability
- Auto
- Life
- Pension
Zen of HIPAA - An employer that sponsors a benefit plan is not a covered entity, but the health plan that it sponsors is a covered entity.

- Legal fiction of separateness within an organization (HR/benefits people and management/workforce)
- Significantly limits flow of information between those in “health plan” box and others, including management/workforce
HIPAA Privacy Standards

- **Administrative Requirements / Notice of Privacy Practices** - impact dependent upon the nature of the plan (insured v. self-insured) and the scope of information that the employer wants to receive from its sponsored health plan.

- **Use and Disclosure** - Health plan can use and disclose PHI only for limited purposes.

- **Individual Rights** - New set of individual rights regarding their PHI.
## HIPAA Privacy Standards - Administrative Requirements

### Self-insured Plans
- Privacy official and complaint contact
- Train workforce and document training
- Implement appropriate administrative, technical and physical safeguards
- Institute internal complaint policy
- No retaliatory acts/waiver of rights to receive benefits
- Monitor systems/document policies

### Fully-insured Plans
- Group health plan does not create or receive PHI, other than summary health information (*i.e.*, non-identifiable, but for 5-digit zip code) and enrollment/disenrollment PHI:
  - No retaliatory acts/waiver of rights to receive benefits
- Group health plan creates or receives PHI for other purposes:
  - Same as self-insured plan
HIPAA Privacy Standards - Notice of Privacy Practices

Self-insured Plans
Group health plan must provide a notice to enrollees in plain language regarding:
- uses and disclosures of PHI
- explanation of individual rights
- details of health plan responsibilities under HIPAA and how to file complaints with HHS

Fully-insured Plans
- Only uses summary health information (i.e., non-identifiable, but for 5-digit zip code) or enrollment/disenrollment PHI:
  - Insurer or HMO must provide notice of privacy practices
- Health plan creates or receives PHI for other purposes:
  - Group health plan must maintain a notice of privacy practices and provide it upon request
• Plan Sponsors (employers) need information for a variety of reasons:
  – Need information to design, price and implement group health plan
  – Need health information for other benefit plans
  – Need health information for ADA, FMLA, sick leave purposes
  – May provide medical services to employees
HIPAA Privacy Standards - Uses and Disclosures
- What is PHI?

- Protected Health Information is information
  - whether oral or recorded, in any form of medium (no longer just electronic)
  - that relates to the individual’s health, healthcare treatment or payment
  - that identifies an individual in any way
  - Broader concept than traditional focus on medical record information
HIPAA Privacy Standards - Uses and Disclosures - Limits

- Group health plan can only use or disclose PHI, absent a specific written authorization from the subject, for
  - treatment, payment or health care operations purposes;
  - for certain public policy related purposes; and
  - where the beneficiary has been told about plan policy of disclosures to certain persons involved in the beneficiaries’ care (right to opt out)
1. **Payment** - coverage decisions, adjudicating claims, performing risk adjustment, billing, processing medical data, COB, eligibility, or conducting UM activities.

2. **Healthcare Operations** - performing QA or QI, credentialing, achieving accreditation or licensure, underwriting and placing insurance, conducting or arranging for medical review, legal services, auditing, including detecting fraud and abuse, business planning and development, business management and general administrative including customer service, internal grievances, and creating de-identified information.

3. **Treatment** - provision, coordination, or management of health care and related services by one or more health care providers (including consultations between providers as to a patient, coordination of care by a provider with a third party, referral from one provider to another).

* FOR EACH OF THE BIG 3, MUST STILL GENERALLY COMPLY WITH “MINIMUM NECESSARY STANDARD”
HIPAA Privacy Standards - Uses and Disclosures - Exceptions

- Marketing Issues
  - Privacy rule permits promotion of terms and conditions of benefit plans

- Payment Issues for Employers: EOBs
  - HHS recognizes that explanation of benefits (EOBs) can contain PHI about the dependants of the employee. HHS notes in the preamble that the employee may be apprised of medical encounters of dependants, but not diagnoses, unless there is an overriding reason (e.g., child suspected of drug abuse due to multiple prescriptions).
“Plan sponsors” are the employers that sponsor or create group health plans for employees, but they are not “covered entities.”

HIPAA’s fundamental concern:
- That the employer will take employment-related actions against an employee based on information that it gets as a result of its role as the plan sponsor.

HIPAA’s solution:
- Create barriers to/conditions upon the flow of health information from the group health plan and/or the TPA to the employer. To get more than very limited PHI, the plan sponsor must amend its plan documents and use the PHI only for plan administration functions specified in the plan documents.
- Employment-related use of PHI requires individual authorization.
Employer access to and use of group health plan PHI is limited:

- Only receive summary health information and it is shared to obtain premium bids from health plans for providing coverage under the group health plan, or to modify, amend or terminate the group health plan;

or

- Employer must satisfy certain operational and documentation requirements to receive additional PHI from its group health plan.
Plan Document Amendments include commitment that Plan Sponsor will:

- certify plan documents have been amended as required;
- only use or disclose for plan administration functions performed on behalf of or for the group health plan and as stated in plan documents or permitted by law;
- ensure that any subcontractors to whom the plan sponsor provides PHI agrees to the same restrictions;
- not use or disclose PHI for employment-related actions or for other benefits or plans;
- make PHI accessible to the subject individual, including allowing subject individuals to amend their PHI;
HIPAA Privacy Standards - Uses and Disclosures - Disclosures to Plan Sponsors/Employers (504(f))

- provide an accounting of disclosures to subject individuals;
- return and destroy PHI when no longer needed, if feasible; and
- ensure firewalls have been established.

- provide adequate firewalls to:
  - identify the employees or classes of employees (by name or function) who will have access to PHI;
  - restrict access solely to employees identified and only for the functions performed on behalf of the group health plan; and
  - provide a mechanism for resolving issues of noncompliance.
HIPAA Privacy Standards - Uses and Disclosures - Business Associates

What is a “business associate”?  
• Entities/persons that perform functions or provide services on behalf of a covered entity including PHI, such as:  
  • claims processing or administration  
  • data analysis  
  • utilization review  
  • quality assurance  
  • billing  
  • benefit management  
  • practice management  
  • repricing  
  • any other activity regulated by HIPAA Administrative Simplification
HIPAA Privacy Standards - Uses and Disclosures - Business Associates

• Any entity/person that provides one of the following services that involves PHI disclosure:
  – legal
  – actuarial
  – accounting
  – consulting
  – data aggregation
  – management
  – administrative
  – accreditation
  – financial services

• Who aren’t Business Associates:
  – members of workforce
  – fully insuring HMO/Issuer (unless additional functions provided not related to the insurance)

• Many plan sponsors whose group health plan has no corporate presence but is simply a plan document/documents administer through TPAs or health carriers. These administrators are business associates and the plan sponsor needs to assure compliance with privacy rules.
HIPAA Privacy Standards - Uses and Disclosures - Business Associates

- Covered Entities must have Written Contracts with Business Associates
- PHI can be disclosed to Business Associates without specific authorization (e.g., a group health plan can disclose to a broker)
- A Covered Entity must take certain actions if it knows of an improper pattern of activity of the Business Associate (mitigate harmful effects)
HIPAA Privacy Standards - Uses and Disclosures
- Business Associates

- Content of Business Associate Contracts:
  - follow same rules the Covered Entity follows
  - not further disclose PHI unless contract permits or law requires
  - report inappropriate uses of PHI
  - require subcontractors to agree to same restrictions
  - make books and records available for inspection by Secretary
  - return or destroy PHI at end of relationship/contract
  - authorize termination if Covered Entity determines Business Associate violated terms.

- If Covered Entity has knowledge of pattern of activity in breach it must take reasonable steps to cure or terminate. If termination is not feasible the Business Associate is to be reported to the Secretary.
• Covered Entities (except for small health plans) that have an existing contract with a Business Associate prior to October 15, 2002 (effective date of rule) are permitted to continue to operate under that contract for up to one additional year beyond the April 14, 2003 compliance date provided that the contract is not modified or renewed prior to that date

  – Note: Covered Entity is permitted to operate under that contract until the earlier of April 14, 2003 or date upon which contract is renewed or modified
HIPAA Privacy Standards - Uses and Disclosures
- Minimum Necessary

• Group health plans (like other covered entities) have to use reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose whenever using or disclosing PHI or requesting PHI from another covered entity

• Disclosures to plan sponsor are governed by minimum necessary requirement
HIPAA Privacy Standards - Individual Rights

- **Access**
  - Right to inspect and copy PHI
  - 30 days (onsite) with 30-day extension

- **Amendment (includes corrections)**

- **Accounting of Disclosures**
  - Other than for TPO and per authorization
HIPAA Privacy Standards - Statutory Penalties

• Criminal penalties: Wrongful Use/Disclosure of Individually Identifiable Health Information
  – Knowingly using a “unique health identifier” or knowingly obtaining or disclosing individually identifiable health information to another person
    • $50,000 maximum penalty,
    • One (1) year maximum imprisonment, or
    • Both
HIPAA Privacy Standards - Statutory Penalties

– Offenses committed under “false pretenses”
  • $100,000 maximum penalty,
  • Five (5) years maximum imprisonment, or
  • Both

– Offenses committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm
  • $250,000 maximum penalty,
  • Ten (10) years maximum imprisonment, or
  • Both
HIPAA Privacy Standards - Compliance and Enforcement

- Department of Health and Human Services ("HHS") empowered to request compliance reports and to undertake periodic compliance reviews.
- No private right of action by an individual created under HIPAA, BUT anyone may file complaints with the Secretary regarding a violation without exhausting any appeals process (e.g., Health plan appeal process).
“As to enforcement, a covered entity will not necessarily suffer a penalty solely because an act or omission violates the rule. As we discuss elsewhere, the Department will exercise discretion to consider not only the harm done, but the willingness of the covered entity to achieve voluntary compliance….Our emphasis will be on education, technical assistance, and voluntary compliance, and not on finding violations and imposing penalties.”
HIPAA Privacy Standards - Compliance and Enforcement

- No private right of action in Federal court - states may have common law theories under which individuals may sue - **BUT MAY CREATE LEGAL STANDARD FOR NEGLIGENCE**
- Enforcement by HHS Office of Civil Rights ("OCR")
- Voluntary Compliance - OCR to provide technical assistance, provide interpretation and guidance
HIPAA Transaction Standards

- Uniform Identifiers assigned to:
  - Individuals
  - Providers
  - Employers
  - Health Plans
- Standard set of codes to be used to encode data elements
- Standard transaction formats for specific types of common transactions
HIPAA Transaction Standards

• Issue:
  – Electronic data interchange (EDI) occurs in over 400 different formats
  – Lack of standardization makes software development difficult and has costs for providers and payors

• HIPAA/HHS Solution:
  – Uniform data elements for 9 transactions
  – Refines existing ANSI x12 standards
HIPAA Transaction Standards

• Rule uses de facto industry standard code sets (a coding system) already in place by most health plans, clearinghouses and providers.

• 8 Standardized Transactions Identified in HIPAA:
  – Health claims or equivalent encounter information
  – enrollment or disenrollment in a health plan
  – eligibility for a health plan (inquiries regarding eligibility, coverage or benefits associated with a benefit plan)
  – health care payment and remittance advice
HIPAA Transaction Standards

• Standardized Transactions (cont’d):
  – health plan premium payments (making and tracking payment of premiums to insurers)
  – health claim status
  – referral certification and authorization for services from a health plan
  – coordination of benefits - transmitting claims and billing payment information between health plans with different payment obligations
HIPAA Transaction Standards

• Does not affect employer as a plan sponsor, only if fall into category of covered entity.
  – Provider (e.g., employee health clinic) - only if file electronically (unlikely)
  – sponsored health plan - must be able to support (burden on insurer/HMO if insured, on TPA if self-insured)

• Covered Entities required to comply with requirements by October 16, 2002 (unless have filed a compliance plan with HHS by October 15, 2002).

• If Compliance Plan filed, have until October 16, 2003 to comply.

• Small health plans have until October 16, 2003, regardless of compliance plan.
HIPAA Implementation

- Client exposure areas
  - reputation/increased media attention
  - private suits
    - traditional privacy
    - employment discrimination
  - Regulatory enforcement
    - HHS/OCR
    - State Attorneys General
HIPAA Implementation - Development of Compliance Response

• Development of Team
  – Legal
    • legal issues
    • attorney-client privilege
  – Consultants - Engage through counsel to cloak in privilege
  – Management and workforce

• Take stock of your group health plans:
  – Insured or Self-Insured and size of plan? (Applicability of HIPAA)
  – Use of TPAs? (Business Associates)
  – What PHI does employer receive?
  – If a covered entity, how will HIPAA compliance be achieved?
HIPAA Implementation - Development of Compliance Response

• What are the goals of the employer as plan sponsor?
  – Management of group health plan?
  – How much PHI is necessary to achieve the goals?
  – Will plan documents need to be modified?
  – Who will develop procedures for “adequate separation” of plan functions, and other administrative requirements?

• Transaction Standards
  – Discussions with Insurer/TPA

• Security?