

HIPAA Privacy: Implications for Pharma, Pharmacies and PBMs



Bruce Merlin Fried, Esq.
For
HIPAA Summit West

June 22, 2001

HIPAA History

- The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)
- Administrative Simplification: Set stage for development of standards for electronic data interchange:
 - Transactions
 - Code Sets
 - Unique Health Identifiers
 - Security Standards
 - Electronic Signatures
 - Transfer of Information Between Health Plans
 - Privacy of Individually Identifiable Health Information



What HIPAA Privacy Means for Pharmas

- Pharma may be a provider
 - If it provides support/guidance on its products to docs or patients (health care), and
 - It conducts standard transactions.
- Pharma subsidiaries may be providers
 - Disease management
 - Specialty Rx and Devices
 - Customized Rx
- Pharma as Business Associate



What HIPAA Privacy Means for Pharmas

- Pharmas will be indirectly impacted
 - Research - Clinical Trials Recruitment
 - Marketing - Impact on DTC
 - Disease management
- Challenges for Pharma Customers
 - Pharmacies, Docs and other Providers
 - Insurers, HMOs, government plans
 - PBMs
 - Patients
- Pharma as an employer



What HIPAA Privacy Means for Pharmacies

- Pharmacies are Providers
- Challenge of Obtaining Consents
- Maintaining Privacy in a Retail Setting
- Implications for Marketing
- Special Challenges for On-Line and Mail Order Pharmacies




What HIPAA Privacy Means for PBMs

- PBMs may be
 - providers
 - Rx dispenser?
 - health plans
 - Risk bearing entity?
 - and/or
- may be Business Associates of plans and providers





The Privacy Rule

- 
- HIPAA required Congress to enact privacy legislation prior to August 1999.
 - Congress failed to act. HHS proposed regulations on November 3, 1999.
 - 54,000 comments were received.
 - Final privacy regulations were published on December 28, 2000.
 - Effective date: April 14, 2001
 - Compliance required within 24 months.

General Rule

- The rule governs the use and disclosure of protected health information (“PHI”) by covered entities which include:
 - Health plans;
 - Health care clearinghouses; and
 - Health care providers who transmit any health care information in electronic form in connection with a transaction covered under the rule.
- Pharma is generally NOT a covered entity.



Definition of PHI

- Protected Health Information is individually identifiable health information (“IIHI”) that is
 - Transmitted by electronic media;
 - Maintained in any medium described in the definition of electronic media in the final transaction and code set regulation; or
 - Transmitted or maintained in any other form or medium.



Definition of IIHI

- IIHI is health information (including demographic information) that is collected from an individual and is:
 - Created or received by a health care provider, health plan, employer or health care clearinghouse;
 - Relates to the past, present, or future physical or mental health condition of an individual; the provision of health care to the individual; or the past, present or future payment for the provision of health care to an individual; and
 - Identifies the individual or creates a reasonable basis to believe the information can be used to identify the individual.



Definition of Health Care Provider

- A health care provider is any person or organization who furnishes, bills, or is paid for medical services or health care in the normal course of business.
- Providers are covered entities only if they transmit any health information in electronic form in connection with a standard transaction or have another entity submit or transmit a standard electronic transaction on the their behalf.
- Pharma May Be a Provider if :
 - It is providing support/guidance on its products to docs or patients (health care) AND
 - It conducts standard transactions.
- PBMs may be Providers if dispensing Rx

ShawPittman



Definition of Health Plan

- A health plan is an “individual or group plan that provides, or pays the cost of, medical care.”
- The definition includes, but is not limited to, 15 different categories of health plans, such as health insurers, HMOs, government plans.
- PBMs may be health plans




Uses and Disclosures

- Required Disclosures
- Permitted Uses and Disclosures
 - Consent
 - Agreement
 - Authorization





Required Disclosures

- 
- Covered entities are only required to disclose PHI under two circumstances:
 - (1) to the individual for inspection and copying or for an accounting; and
 - (2) when required by the Secretary for compliance purposes.

Permitted Uses/Disclosures

- A covered entity *may use or disclose* PHI as follows:
 - With permission of the individual in the form of consent, authorization, or agreement;
 - Without permission
 - to the individual,
 - for judicial and administrative proceedings,
 - for law enforcement purposes,





Permitted Uses/Disclosures

- A covered entity *may use or disclose* PHI without permission:
 - For public health activities, including for disclosure to an entity subject to FDA regulation to report adverse events, enable product recalls, etc.
 - For Research purposes provided that:
 - IRB or privacy board approves waiver from authorization requirement,
 - researcher represents that use of PHI is solely to prepare research and will not be used otherwise.



Consent

- Required. Health care providers with direct treatment relationships are required to obtain written consent from the individual prior to using or disclosing PHI for treatment, payment or health care operations with certain exceptions (e.g., emergency care).
- Permitted. Other covered entities may obtain consent for such purposes but they must comply with consent rule if they decide to obtain consent.



Definitions

- Treatment: the provision, coordination or management of health care and related services by one or more health care providers. [Disease management for an individual may be “treatment”.]
- Payment: the activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or a covered health care provider or health plan to obtain or provide reimbursement for the provision of health care; and these activities relate to the individual to whom health care is provided.
- Health care operations:
 - (1) Conducting quality assessment and improvement activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;



Definitions

- Health care operations (continued):
 - (2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
 - (3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care, provided certain requirements are met;
 - (4) Conducting or arranging for medical review, legal services, and auditing functions;
 - (5) Business planning and development; and
 - (6) Business management and general administrative activities of the entity.



Consent Requirements

- Must be in plain language and must:
 - Inform the individual that PHI may be used/disclosed to for treatment, payment or health care operations; and
 - State that
 - the individual has the right to request that the provider restrict how PHI is used/disclosed to carry out treatment, payment or health care operations,
 - the provider is not required to agree to requested restrictions, and
 - that if the provider agrees to such restrictions that the restriction is binding.



Consent for Pharma, PBM, Pharmacies

- Pharmacies must obtain consent -- provider with a direct treatment relationship.
- PBM -- If directly dispensing to patient, then a provider with a direct treatment relationship, must get consent.
- Pharma -- is it a provider? Does it have a direct treatment relationship?





Consent for Pharmacies

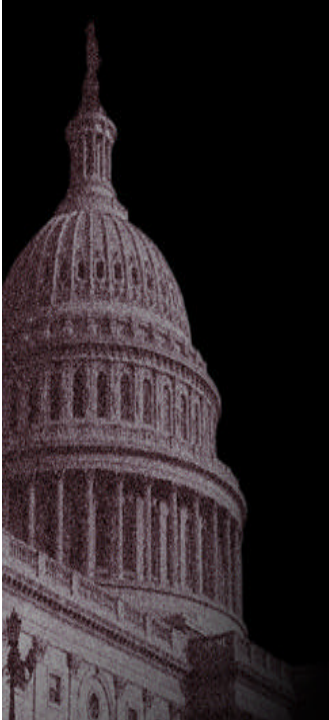
- Obtaining consents from Pharmacy patients presents special challenges
 - Consumers may go to multiple pharmacies
 - Some patients never go to the pharmacy, friends or family or delivery
 - Administrative challenge for pharmacies with large numbers of customers
 - What about patient buying OTC on pharmacist recommendation? Is consent needed?



Agreement or Objection

- Agreement, verbal, is required in two circumstances:
 - (1) for facility directories; and
 - (2) to people involved in the individual's care and notification purposes.
- Under this provision, the individual generally must be informed in advance of the use or disclosure and have the opportunity to agree or prohibit or restrict the disclosure.





Agreement or Objection for Pharmacies

- Is Agreement required when friends or family pick up your Rx?
- May be informal and implied from the circumstances



Authorization

- Authorizations are required for any use or disclosure that is not permitted under the rule or for which consent or agreement are not required.
 - PHI may not be used for marketing without Authorization



Authorization Requirements

- All authorizations must be written, in plain language and include certain provisions, such as:
 - A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
 - An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure; and
 - A statement that information used or disclosed pursuant to authorization may be subject to redisclosure by the recipient and no longer be protected by the rule.



Indirect Regulation

- Although the Secretary only has the authority to directly regulate covered entities, the rule *indirectly* regulates many noncovered entities by conditioning disclosure of information by the covered entity on contractual relationships with these other entities known as “business associates.”



Business Associate - Definition

- A business associate is:
 - (1) a person who uses or discloses PHI to perform a function on behalf of a covered entity, or
 - (2) a person who provides the following services to a covered entity: legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial services.



Business Associates

- Covered entities are required to contract with business associates except, among other reasons, for disclosures by a covered entity to a health care provider concerning the treatment of an individual.
- The contract must contain certain provisions, such as:
 - The business associate may use or disclose PHI only as allowed under contract and may not use or disclose PHI in a manner that would violate the rule if performed by the covered entity, with exceptions; and
 - The business associate must use appropriate safeguards to prevent the use or disclosure of information other than as provided for by its contract.



Monitoring of Business Associates

- A covered entity that has knowledge of a “pattern of activity or practice of the business associate that constituted a material breach or violation” of the business associate’s contract, must take “reasonable steps to cure the breach or end the violation.”
- If such steps are unsuccessful, the covered entity must terminate the contract, if feasible, or, if termination is not feasible (e.g., unreasonably burdensome due to a lack of alternatives), report the problem to the Secretary.
- A covered entity is not required to actively monitor a business associate but must investigate complaints.



Minimum Necessary Standard

- When using or disclosing or requesting PHI from a covered entity, the covered entity must make reasonable efforts to limit PHI to the minimum amount necessary to accomplish the intended purpose.
- This standard does not apply, among other reasons, when disclosing to, or when requested by, providers for treatment.
- Covered entities are required to have policies and procedures governing the use and disclosure of and requests for PHI. For some types of disclosure and requests, a case-by-case determination of what is minimally necessary is required.



Individual Rights

- Notice
- Request restriction
- Access
- Amendment
- Accounting



Notice

- Standard. An individual has a right to adequate notice of the uses and disclosures of PHI that may be made by the covered entity, and of that individual's rights and the covered entity's legal duties with respect to PHI.




Content of Notice

- Must be in “plain language” and contain certain elements such as:
 - Header. “This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.”
 - Uses and Disclosures. In general, the covered entity must describe all of the types of uses and disclosures permitted or required by law (not just those it intends) to make.



Right to Request a Restriction



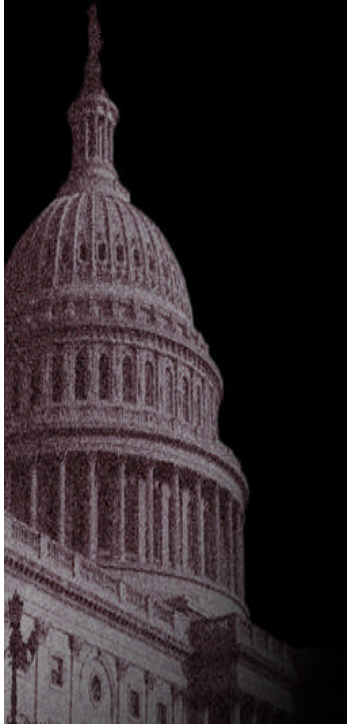
- Standard. A covered entity must permit an individual to request that the covered entity restrict uses or disclosures of PHI for treatment, payment, and health care operations, as well as uses and disclosures for involvement or assistance with the individual's care and notification.

- If the covered entity agrees to such restriction, it must abide by the restriction with certain exceptions. For example, If a covered entity agrees to the request "not to disclose PHI to my sister," a covered entity cannot disclose PHI to the sister even if otherwise permissible.

ShawPittman

Access of Individuals to PHI

- Standard. An individual has a right of access to inspect and obtain a copy of the health information about the individual in a designated record set, for as long as the PHI is maintained in the designated record set (with certain exceptions).
- A designated record set is a group of records maintained by the covered entity that is used, in whole or in part, by or for the covered entity to make decisions about individuals.





Amendment of PHI

- Standard. In general, an individual has the right to have a covered entity amend PHI or a designated record set for as long as the PHI is maintained in the designated record set.



Accounting

- Standard. An individual has a right to receive an accounting of disclosures of PHI made by a covered entity or business associate in the six years prior to the date on which the accounting is requested.





Administrative Procedures Imposed on Covered Entities

- A covered entity must perform certain administrative procedures, such as:
 - Designate a privacy officer;
 - Designate a contact person;
 - Provide privacy training for all employees;
 - Implement safeguards to prevent intentional or accidental misuse of PHI; and
 - Provide a process for individuals to make complaints.

State Privacy Laws

- State Privacy laws preempt HIPAA where they are more stringent than and not in conflict with HIPAA .
- Very complex analysis required for multi-state insurers and providers.
- Shifting sands, more than 2,000 state bills were introduced this year alone.





ShawPittman

where LAW,
BUSINESS and TECHNOLOGY converge

Providing Comprehensive Legal Services
for the Health Care Community

Bruce.Fried@shawpittman.com

202-663-8006

2300 N Street, NW

Washington, D.C. 20037

Washington Northern Virginia New York

Los Angeles London



ShawPittman