

The HIPAA Privacy Rule: Is Your Health Plan Ready?

[Mary E. Copper](#)
[Jennifer Gimler Brady](#) [1]

What is HIPAA?

- The Health Insurance Portability and Accountability Act of 1996.
- HIPAA was enacted to simplify the administration of health insurance.
- It also requires the development of privacy regulations designed to protect medical records and other “protected health information” [“PHI”].

Requirements – Application Originally

HIPAA was intended to apply only to electronic records and not paper records. However, the final rule indicates that the HIPAA privacy rule applies to “all individually identifiable health information transmitted or maintained by a covered entity regardless of form.”

The Final Privacy Rule

The compliance deadline for small health plans (receipts of \$5 million or less) is April 14, 2004.

Who is covered by the Privacy Rule?

- Health Plans (e.g., employee welfare benefit plans, health insurance issuers and HMOs).
- Health Care Clearinghouses (e.g., re-pricing companies, billing companies and value-added networks).
- Health Care Providers (e.g., doctors, hospitals, long-term care facilities, home health agencies, etc.) who transmit PHI in electronic form.

What is PHI?

- PHI is information created or received by a health care provider, health plan, employer or health care clearinghouse that relates to an individual’s past, present or future health or condition.
- Generally covers individuals Identifiable Health Information [“IHI”].
- Any form of PHI – verbal, written or electronic – is covered.

- *Is in the possession or control of a covered entity (including a group health plan).*

Identifying PHI

- Does the information identify the individual or is the individuals' identity readily discernable from the information?
- Does the information relate to the past, present or future physical or mental health condition, the provision of health care to an individual or payment for health care?
- Was the information created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university or health care clearinghouse?

Who must protect PHI?

- Covered entities – including group health plans – must protect the confidentiality of PHI.
- A group health plan must implement policies and procedures to protect PHI.

What is a Covered Group Health Plan?

- Employee plan covered by ERISA;
- Insured or self-insured;
- Provides medical care, including items and services paid for as medical care to employees or dependents directly or through insurance, reimbursement or otherwise;
- Has 50 or more participants or is administered by an entity other than the employer that established the plan.

Covered Group Health Plans:

Examples:

- Fully insured employer health plans – regardless of the number of participants.
- HMO
- Health flexible spending accounts (health “FSA”)
- Employee Assistance Plan (“EAP”).
- Long-term care plan.

Not Covered:

- AD&D
- STD and LTD
- Life insurance
- Workers' Compensation
- Coverage for on-site clinics
- Liability insurance
- Liability insurance supplements
- Automobile medical payment coverage
- Credit only insurance

**Privacy Rule:
Compliance Overview**

- Limiting the uses and disclosures of PHI;
- Enforcing individual rights with respect to PHI;
- Providing a notice of privacy practices;
- Amending plan documents to permit disclosures and uses of PHI for purposes of plan administration; and
- Administrative requirements – appointment of a privacy official, implementing safeguards, and training employees.

**Group Health Plans:
Insured v. Self-Insured**

- Insured status may make a significant compliance difference.
- Generally, a fully-insured plan (“FIP”) that receives only limited information about participants will have a lighter compliance burden.
- Insurers and HMOs will have the compliance burden for fully-insured plans.
- Self-insured plans (“SIP”) are presumed to receive PHI and will have a significant compliance burden.

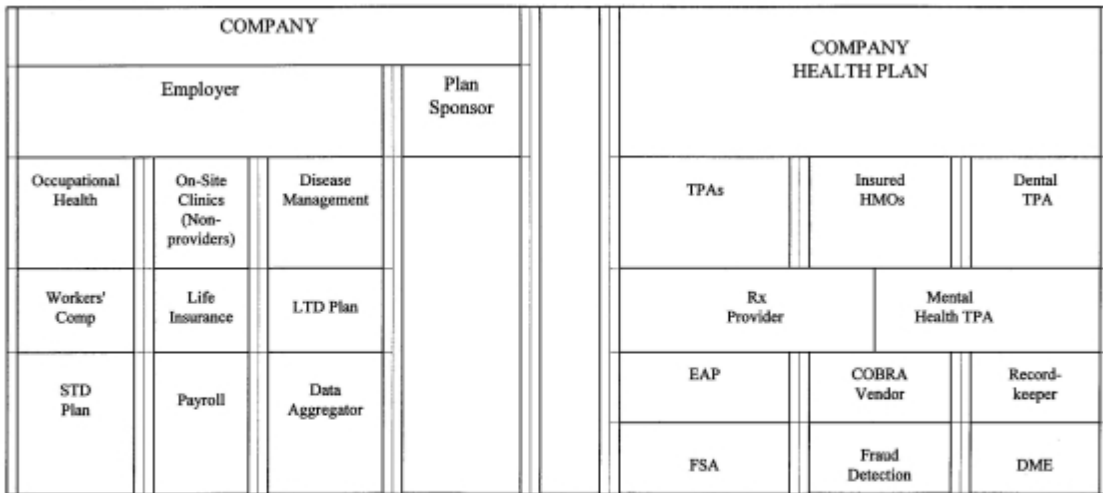
**Group Health Plan Compliance:
Analytical Framework**

- A group health plan is treated as completely separate from the employer for purposes of the Privacy Rule.
- The employer is treated essentially as two different entities:
 - Plan sponsor; and
 - Employer (all other functions)

**Group Health Plans:
Employer as Plan Sponsor**

- Consists of those employees who perform plan administration or “settlor” functions.
- Employees may “wear two hats”, if they spend part of their time performing plan administrative functions and part performing other functions.

**Diagram:
Employer/Plan Sponsor/Health Plan**



Privacy Rule Compliance

1. Limiting Use and Disclosure of PHI

Requirements – Patient/Employee Authorization

A covered group health plan must secure an authorization to disclose PHI, unless disclosure is required or otherwise permitted by the Privacy Rule.

Required Disclosures

When the participant or beneficiary who is the subject of the PHI requests it. When HHS requests access to investigate or determine compliance with the Privacy Rule.

Uses and Disclosures Permitted Without Permission of Individual

- To the individual that is the subject of PHI;
- For treatment, payment and healthcare operations;
- To a service provider under a “business associate” agreement
- For certain specified uses and disclosures; and
- Incidental to other permitted or required uses and disclosures if “minimum necessary” rule satisfied.

Minimum Necessary Disclosure

- Covered entities must use reasonable efforts to prevent disclosure beyond that necessary to accomplish purpose
- Exceptions
 - Disclosures to the patient
 - Disclosures to the Secretary of HHS
 - Other permissible disclosures required by law

Minimum Necessary Use

- Covered entities must identify persons in the workforce who need access to PHI
- Covered entities must identify categories of PHI needed for each person or class and conditions appropriate to access

TREATMENT

Treatment means the provision or coordination of health care by or among health care providers.

PAYMENT

Payment includes activities aimed at obtaining premiums, determining or fulfilling responsibilities for coverage under a health plan, or obtaining reimbursement.

Health Care Operations

- General administrative and business functions necessary for the group health plan to conduct its business;
- Minimum necessary requirement applies to uses and disclosures for health care operations activities.

Permitted Disclosures by Group Health Plan to Plan Sponsor: Plan Administration

- Only to employees functioning as plan administrator and only for purposes of plan administration.
- Requires plan amendments to reflect and restrict uses and disclosures of information.
- Only minimum necessary may be disclosed.

**Permitted Disclosures by Group Health Plan to Plan Sponsor:
For “settlor” functions**

May disclose PHI in the form of “summary health information”, if the employer requests it, for the purpose of modifying, amending or terminating the plan or procuring bids from other health plans for health insurance coverage.

**Permitted Disclosures by Group Health Plan to Plan Sponsor:
Participation & Enrollment Information**

- May disclose PHI in the form of participation, enrollment and disenrollment.
- No plan amendment required.
- Minimum necessary requirement applies.

**Permitted Disclosures by Group Health Plan to Plan Sponsor:
De-identified Information**

May disclose de-identified information to plan sponsor, the employer or any other party because de-identified information is not PHI and not subject to the Privacy Rule.

Other Disclosures Permitted without Individual Authorization

- To the individual that is the subject of the PHI;
- For treatment, payment and health care operations of another covered entity;
- To a service provider under a “business associate” agreement;
- Disclosures about victims of abuse, neglect, or domestic violence;
- Disclosures for judicial and administrative proceedings;
- Uses and disclosures required by law, for health oversight activities or law enforcement purposes;
- Relating to decedents;
- For research;
- Relating to military personnel;
- For workers compensation
- For tissue and organ donations
- To avert a serious threat to health or safety;
- Relating to national security and intelligence operations;
- To the personal representative

Requirements – Participant Authorization When Required

- Must have authorization for any use or disclosure not recognized by regulations.
- Need authorization for ANY use of psychotherapy notes (except: for use by the originator for treatment; use in in-house training; or defense in legal action brought by the subject of the PHI)
- Authorization must be separate from other documents, such as a notice of privacy practices.

Participant Authorization – Core Elements

- A description of the information to be used or disclosed.
- The identification of the information to be used or disclosed.
- The identification of the persons or class of persons permitted to make the use or disclosure.
- The identification of the persons or class of persons to whom the covered entity is permitted to make the use or disclosure.
- An expiration date or event upon which the authorization will expire.
- Individual's signature / statement of authority to sign.

Participant Authorization – Notification Requirements

- A statement that the authorization may be revoked in writing and a description of the revocation process.
- A statement that treatment, payment, enrollment and eligibility for benefits may not be conditioned on the authorization.
- A statement that PHI may be subject to re-disclosure.

2. Enforcing Individual Rights with Respect to PHI

Right to Request Privacy Protection –Uses and Disclosure

- Request that the group health plan restrict its uses and disclosures of PHI in carrying out payment and health care operations;
- Includes disclosures made to family members and those involved in care.

Refusal or Termination of Request

- Plan is not required to agree to request.
- Plan may unilaterally terminate a restriction;
- Unilateral termination applies only to PHI received after notification or termination.

Documentation Requirements

- Agreed-upon restrictions must be documented;
- Agreed-upon termination must also be documented.

Right of Access

- A group health plan must permit a participant or beneficiary to inspect and get a copy of certain PHI in the plan's "designated record sets".
- Subject to certain exceptions.

"Designated Record Sets"

- Enrollment, payment, claims adjudication and case or medical management records systems maintained by or for the plan;
- All other records used, in whole or in part, by the plan to make decisions about participants and beneficiaries.

Right of Access – Exceptions

- Not in plan's possession;
- Not in "designated record set";
- Safety reasons;
- Psychotherapy notes;
- Compiled by or on behalf of the plan in connection with legal proceeding;
- Denial is proper under Privacy Act;
- Obtained from outside source in confidence.

Right to Request Amendment

- Participants and beneficiaries have the right to request amendments to their PHI held by the plan;
- Plan must generally comply if it determines that the records at issue are not accurate and complete.

Right to an Accounting

Participants and beneficiaries have the right to request an accounting of certain disclosures of their PHI made by the plan.

Requests for Amendments – Denial

- Denials must be communicated in a writing that explains:
- The reason(s) for the denial

- The patient's right to "appeal" the denial
- The patient's right to request attachment of the amendment request and denial to future disclosures of PHI
- How to complain about the denial

3. Notice of Privacy Practices

Notice of Privacy Practices

A notice of privacy practices is a document that summarizes how a group health plan uses and discloses PHI and an individual's rights with respect to PHI.

Group Health Plans: Privacy Notices

- All self-insured plans must create, maintain and distribute a notice of privacy practices.
- Fully-insured plans do not have to distribute a notice of privacy practices but must prepare and maintain a notice if they receive PHI.

Group Health Plans: Privacy Notices

- Fully-insured plans that receive only SHI and enrollment/disenrollment information do not have to prepare or distribute a notice of privacy practices.
- The insurer or HMO will be required to issue the notice of privacy practices.

Right to Request Privacy Protection - Alternative Communication

- Participants may request alternative means of communicating PHI
- Plans must agree to request if it is "reasonable"

4. Amending Plan Documents

Plan Amendments Required

- If the plan sponsor receives PHI in order to continue to perform plan administrative functions.
- Applies to both fully-insured and self-insured plans.

No Amendment Required

- Plan sponsor receives no PHI;
- Plan sponsor receives only SHI which is used only for obtaining premium bids in connection with modifying, terminating or amending plan;

- Plan sponsor receives only participation and enrollment information.

5. Administrative Requirements

Administrative Requirements – Privacy Official

- SIP and FIP (w/ PHI) must appoint a privacy official who is responsible for developing, implementing and monitoring privacy policies and procedures (could be FT or PT)
- Also must designate a privacy contact to receive complaints / explain policies (may be same person as privacy official for smaller entities)

Administrative Requirements – Privacy Policies and Procedures

- SIP and FIP (w/PHI) must develop, implement and document privacy policies and procedures
- Procedures must incorporate patient rights (i.e., access, copying, amendment, etc.)
- Procedures must provide for sanctions on workforce members who use PHI in violation of the privacy regulations.

Administrative Requirements – Training

- SIP and FIP (w/PHI) must provide privacy training to the plan workforce on the policies and procedures required by the regulations to protect PHI.
- Must be appropriate to job functions
- Re-training must be provided
- Training must be documented

Administrative Requirements – Privacy Safeguards

- SIP and FIP (w/PHI) must adopt administrative, technical and physical safeguards to protect PHI
- Examples
 - Locked file cabinets and file rooms that house PHI
 - Shredding documents that contain PHI before disposal

Administrative Requirements – Complaint Process

- SIP and FIP (w/PHI) must create a process for receiving complaints regarding possible violations of privacy protections
- All complaints and actions taken must be documented (retain for 6 years)

Administrative Requirements – No Retaliation

- Cannot retaliate against any person who exercises the privacy rights granted under the HIPAA regulations
- Protection applies to insured, insured's relative, employee or business associate

Administrative Requirements – Sanctions

- SIP and FIP (w/PHI) must have procedures in place to measure compliance with privacy policies
- Also must have policies and procedures to impose appropriate sanctions for violations by employees or business associates
- Violations / sanctions must be documented
- Can't sanction a whistleblower

Administrative Requirements – Mitigation

- SIP and FIP (w/PHI) must have procedures in place to lessen the harmful effects of violations of privacy policies or procedures.
- Mitigation activities may include:
 - Notification of affected person
 - Retrieval if feasible
 - Prevention of future violations, including policy modifications, limiting disclosures, etc.

Administrative Requirements – No Waiver

Covered entities may not require, as a condition of treatment, payment, enrollment or eligibility for benefits, that an individual waive the right to lodge or pursue a complaint regarding privacy violations.

Administrative Requirements – Business Associate Agreements

In order to disclose PHI to a person, business or other entity who, on behalf of the plan, performs or assists in a function or activity involving the use or disclosure of PHI, the plan must enter into an agreement with the "Business Associate".

Business Associate – Examples of Functions

- Claims processing or administration
- Data analysis
- Utilization review and quality assurance
- Billing and benefit management
- Practice management

- Re-pricing
- Legal, accounting, actuarial, consulting, management, accreditation or financial services

Administrative Requirements – Business Associate Contracts

- Must have business associate contracts signed by compliance deadline
- Contract requirements:
 - List permitted uses and disclosures of PHI that business associate may make
 - Prohibit use or disclosure except as permitted by contract or authorized by law
 - Include appropriate safeguards to prevent misuse or inappropriate disclosure of PHI
 - Include reporting obligation re: violations
 - Require business associates to impose same obligations on subcontractors and agents
 - Require business associates to make PHI available for access, copying, and amendment
 - Require business associates to assist the covered entity in providing an accounting of disclosures of PHI
 - Require business associates to make practices, books and records available for HHS review
 - Require business associates to return or destroy PHI upon termination of contract
 - Provide for termination of agreement in the event of a material breach (which should include a material violation of the privacy regulations)

Penalties for Non-Compliance

- Secretary of HHS has authority to impose penalties for non-compliance
- Enforcement authority has been delegated to the Office of Civil Rights
- \$100 per violation up to an annual maximum of \$25,000
- Courts may impose criminal penalties of up to \$250,000 and/or up to 10 years in jail for certain intentional privacy violations

Entity Costs

- Analysis of rules and impact on entity
- Development and documentation of policies and procedures
- Changing or developing systems
- Dissemination of policies and procedures
- Training
- Compliance / personnel requirements

- Obtaining consents and authorizations

Preemption

- HIPAA preempts state laws that are contrary to or in conflict with the privacy regulations' requirements
- State laws that are more restrictive or stringent are not preempted by the HIPAA privacy regulations
- Compliance can be complicated and expensive for multi-jurisdictional entities

PHI Received by employer in capacity as employer.

Q: Is all PHI received by an employer subject to the Privacy Rule?

A: No. Only PHI received or maintained by the employer as plan sponsor is subject to the Privacy Rule.

Examples of Actions Not Subject to Privacy Rule

- PHI collected by employer for purposes of drug testing, pre-employment physicals and fitness-for-duty examinations is not subject to the Privacy Rule.
- Important distinction: PHI is not received from group health plan.

Complications for Employers – Obtaining Information

- An employer may have difficulty obtaining information from employees' medical providers;
- Medical providers are covered entities and will want authorization forms.

Complications for Employers – Workers Compensation

- HIPAA regulations specifically authorize covered entities to disclose PHI to the extent necessary to comply with workers compensation laws;
- Workers compensation carriers, IAB and employers can get PHI without employee authorization;
- Employees cannot rely on HIPAA to resist information requests regarding illness-related leaves of absence.

Substantiating claims for sick leave, etc.

Q: Can the employer require doctors' notes to establish the need for paid sick leave, or in connection with FMLA, ADA, etc.?

A: Yes – but the medical professional may require the employee's authorization.

Are On-site Clinics Covered?

An employer that provides health care to its employees in kind will be a “covered health care provider”, even though it does not bill its employees or require payment for the services, if it transmits any health information in electronic form in connection with specified types of transactions.

Notes:

- 1 The views expressed in this presentation are those of the authors and may not reflect the views of Potter Anderson & Corroon LLP or its clients. Nothing in this website or the publications included in this website is intended to create an attorney-client relationship. This presentation should not be deemed legal advice and should not be relied on by you as legal advice related to your particular circumstances.