October 29, 2020

HIPAA Privacy & Security & The Employer

Hays
PART OF THE BROWN & BROWN TEAM

+

Brown & Brown INSURANCE

Disclaimer

This presentation is provided for general information purposes only and should not be considered legal or tax advice or legal or tax opinion on any specific facts or circumstances. Readers and participants are urged to consult their legal counsel and tax advisor concerning any legal or tax questions that may arise.

Any tax advice contained in this communication (including any attachments) is not intended to be used, and cannot be used, for purposes of (i) avoiding penalties imposed under the U. S. Internal Revenue Code or (ii) promoting, marketing or recommending to another person any tax-related matter.

Privacy & Security Presentation

This presentation is intended to augment your employer's HIPAA privacy and security policies and procedures as well as any other information provided to you regarding HIPAA privacy and security requirements.

It is you responsibility to be familiar with your company-specific polices and procedures.

HIPAA Privacy & Security Overview

HIPAA Privacy & Security

Health Insurance Portability and Accountability Act of 1996

- Set standards for privacy and security of protected health information.

PRIVACY

limits the circumstances and people that can access, use or disclose PHI

SECURITY

the mechanisms and safeguards used to prevent unauthorized access to EPHI

The Regulated Community

Covered Entities:

- Health plans
- Health care clearinghouses
- Health care providers conducting electronic transactions

Business Associates:

- Their-party claims administrators
- Consultants and analysts
- Brokers/agents
- Attorneys

The employer is not the covered entity – the group health care plan is the covered entity – this is about the group health plan, dental plan, vision plan, health FSA, HRA etc.

The Regulated Information

Protected Health Information (PHI)

Health Information (HI) + **Individually identifiable health information (IIHI)** + **Used or disclosed by a covered entity**

=

Protected health information (PHI).
If in electronic format = EPHI

Examples of PHI

- Bill for health services.
- Explanation of Benefits (EOB) statement.
- Receipts and/or submissions for medical flexible spending account reimbursements.
- Health FSA or HRA reports listing reimbursement amounts.
- Documentation provided by an employee to the health plan to prove that benefits should be paid.
- Lists showing benefits paid broken down by social security number.
- Enrollment and disenrollment information maintained by the plan or carrier (limited employer exception).

Basic Requirement – Privacy

The Covered Entity must:

- Implement appropriate administrative, technical, physical and organizational safeguards to protect the privacy of PHI.
- Adopt privacy policy and procedures
- Mitigate any harmful effect of a use or disclosure of PHI in violation of its policies and procedures or the Privacy Rule that is known to the Covered Entity, to the extent practicable.

Although the employer is not the “covered entity” the employer is responsible for the plan and therefore must ensure the privacy requirements are satisfied.

Basic Requirement – Security

Covered entities must ensure the confidentiality and integrity, and availability of Electronic Protected Health Information (EPHI).

A covered entity must develop policies and procedures that:

- Protect against reasonably anticipated threats or hazards to the security of EPHI;
- Protect against reasonably anticipated uses and disclosure of EPHI that is not permitted or required;
- Ensure that its workforce complies with the requirements of the Security Standards.

Covered entities with EPHI need to appoint a Security Official to oversee the HIPAA Security program.

Privacy & Security

Administrative Safeguards

Policies and procedures used to manage selection, development, implementation, and maintenance of security measures to protect EPHI and to manage the conduct of the covered entity's workforce in relation to EPHI.

Physical Safeguards

Physical measures, policies, and procedures designed to protect a covered entity's electronic information systems, and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Privacy & Security

Technical Safeguards

The technology, and the policy and procedures for its use, that protects EPHI and controls access to it.

Organizational Safeguards

The covered entity may permit business associates to receive, maintain, or transmit EPHI if satisfactory assurance is obtained that the business associate will safeguard the information.

System Security

- Email Procedures
- Remote Access Controls
- Disaster Recovery Procedures
- Segregating data
- Virus/Spam Protection /Context Filters
- Encrypted laptops & removable devices

- Firewalls & Encryption
- Password Protection
- Auto Logoff Procedures and Confidentiality Reminder
- Stronger Server Access Control
- Backup Systems

Breach

Breach:

An unauthorized acquisition, access, use or disclosure of Protected Health Information (PHI) that compromises the information's security or privacy in a manner not permitted under the privacy rule.

Exceptions:

- No retention of information
- Certain good faith disclosures
- Certain internal disclosures

Applicable to Covered Entities and Business Associates.

Secured & Unsecured PHI

Secured PHI

- PHI that is rendered Unreadable, Unusable or Indecipherable
  - Encryption or destruction
- Encrypted electronic PHI does not require a risk assessment or breach notification.

Unsecured PHI

- PHI that is not secured by using a technology or methodology specified by HHS.
- Unsecured PHI is presumed to be compromised.

Breach Risk Assessment

Determining whether a breach occurred requires a risk assessment.

- ✓ The nature and the extent of PHI involved;
- ✓ The unauthorized person who used the PHI or to whom the PHI was disclosed;
- ✓ Whether the PHI was actually acquired or viewed; and
- ✓ The extent to which the risk to PHI has been mitigated.

Notification Requirements

Covered entities must notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired or disclosed as a result of a breach.

- Notice must be provided to each affected individual via first-class mail at the individual's last known address, or
  - May be by e-mail if the individual specifically indicated a preference for e-mail notices.
- Notice must be provided without unreasonable delay.
  - In no case later than 60 calendar days after the breach is discovered.

If more than 500 records have been breached, notice to the media is required. In addition, HHS must be notified.

Employer as Plan Sponsor

Three Levels of Employer Records

Individually Identifiable Information

Level 3	Medical information from group health plan or health care provider – HIPAA Privacy & Security for Protected Health Information (PHI).
Level 2	Medical information in role as employer - FMLA, workers' compensation, ADA, drug & alcohol testing, sick leave, disability plans, fitness-for-duty records, OSHA, DOT.
Level 1	Personnel records - date of hire, promotions, discipline, etc.

Employer / Plan Sponsor

TPO = **T**reatment, **P**ayment, Health Care **O**perations

Inside the TPO Universe

Group Health Plan

Third-party Claims Administrator

Clinic

Insurance Company

Hospital

HMO

PPO

PHI may be used or disclosed within the Universe for TPO purposes without authorization

Outside the TPO Universe

Enrollment & disenrollment

Marketing Organization

Disability Insurance

Workers' Compensation

Life Insurance

Employer / Plan Sponsor

When the covered entity is the group health plan, an employer may be obligated to comply with the HIPAA privacy rule in its role as the plan sponsor.

Employers will have HIPAA privacy rule responsibilities when they:

- Have a self-insured group health plan, or
- Participate in the administration of a group health plan, or
- Are active in the decision-making process of a group health plan, or
- Participate in the operation or control of the provisions of a group health plan.

Employer – Plan Sponsors & PHI

The plan sponsor is not a covered entity

- But PHI may be necessary for health care plan operations.*
  - Plan administration = claims processing, quality assessments, claims management, auditing and monitoring.

For employees of the plan sponsor to receive PHI:

- Obtain individual authorization each time, or…
- Plan documents may be amended to allow this type of disclosure of PHI.

*Quality assessments, health improvement activities, underwriting or premium rating, performance or arrangement of audits and legal services, business planning and management, creation and provision of aggregate data for analysis, resolution of initial grievances, and due diligence in corporate transactions.

Hays PART OF THE BROWN & BROWN TEAM + Brown & Brown INSURANCE

Authorization

For disclosure other than for treatment, payment or health care operations, the covered entity that has the PHI must obtain an authorization from the individual to whom the PHI pertains.

Example: employee applies for a disability benefit; underwriting for excess life insurance, etc.

- **PHI may be disclosed for any purpose authorized by the individual.**
- **The authorization must be specific.**

De-Identifying PHI

The Privacy Rule allows a covered entity to freely use and disclose information that neither identifies nor provides a reasonable basis to identify an individual.

The Privacy Rule's standard for de-identifying PHI recognizes the following de-identification methods:

- A formal determination by a qualified expert (Expert Determination Method); or
- The removal of specified individual identifiers as well as absence of actual knowledge by the covered entity that the remaining information could be used alone or in combination with other information to identify the individual (Safe Harbor Method).

Administrative Requirements

These are the requirements that an employer, as plan sponsor of a covered entity, must ensure are in place:

1. Privacy Official & Security Official
2. Perform a risk analysis regarding any ePHI that the group health plan creates or receives.
3. Policies & procedures
4. Designated contact person (may be privacy official)
5. Train employees
6. Establish a participant complaint process
7. Apply appropriate sanctions
8. Provide the Privacy Notice
9. Implement Business Associate Agreements

Privacy Notice Requirements

Describes:

- The uses and disclosures of PHI
- Individual rights & covered entity's duties
- Complaints & contact information

Responsibility:

- If fully insured – issuer responsibility (If the sponsor of a fully insured plan is hands-on PHI, it is required to maintain a Privacy Notice and to provide the notice upon request).
- If self insured – plan responsibility.

✓ Notice must be sufficiently detailed to inform individual of privacy practices.

✓ Provide upon coverage under the plan.

- Reminder notice every three years.
- If fully insured, must inform participants that a notice is available through the carrier.

Privacy Notice Requirements

Distribution Deadlines:

- At least once every three years, (or notify participants that the notice is available and how to obtain a copy).

- In addition, health plans must provide the Privacy Notice in the following circumstances:
  - To new enrollees at the time of enrollment;
  - Within 60 days of a material change to the notice (see below for more information and a special exception under the final rule); and
  - Any time upon a participant's request.

- If a health plan sends out a revised notice (for example, following a material change to the notice), it will reset the three-year notice requirement.

Employer / Plan Sponsor

Employees of the employer/ plan sponsor may:

- ✓ Receive summary health information for limited purpose use (health plan operations).
- ✓ Enroll and dis-enroll participants and make payroll deductions.
- ✓ Assist employees with understanding their plans.

Employer / Plan Sponsor

Employees of the plan sponsor may assist an employee with claim issues.

Example: an employee asks the employer's benefits manager for help understanding an explanation of benefit form (EOB).

- The benefits manager may contact the provider, insurance company or plan administrator on behalf of the employee.
- If the benefits manager needs additional PHI from the provider, insurance company or plan administrator, that entity must obtain authorization from the employee (it is the covered entity's responsibility).

Employer / Plan Sponsor

Employers may not:

- ✓ Intimidate or retaliate against a person who;
  - Exercises their privacy rights
  - Files a complaint
  - Participates in an investigation
  - Opposes any improper practice under HIPAA

When HIPAA Does Not Apply

Not all individually identifiable health information is regulated by HIPAA privacy & security rules.

- **Life insurance records**
  - The insurance carrier is not a covered entity
- **Disability coverage records**
  - The insurance carrier is not a covered entity
- **Although individual identifiable health information is used, it is obtained directly form the individual or by authorization of the individual**
  - If you are collecting this information, treat as confidential

When HIPAA Does Not Apply

ADA & FMLA records typically include medical information.

- Documents relating to medical certification and recertification of employees (or family members) must be kept as confidential medical records separate from personnel files.
  - Supervisors and managers may be informed of restrictions and necessary accommodations.
  - First aid and emergency personnel may receive medical information if the disability may require emergency treatment.
  - Government officials investigating claims may receive relevant medical information.

When HIPAA Does Not Apply

Not regulated by HIPAA:

- **Employment records**
- **Workers' Compensation**
- **OSHA records**
- **Drug & alcohol testing**

Under one of HIPAA's public health exceptions, health care providers that are providing services at the request of an employer relating to worksite injuries or workplace-related medical surveillance may disclose to the employer limited information that the employer needs to comply with occupational safety and health laws as well as mine safety and health laws, or similar state laws, so long as certain requirements (e.g., providing notice of the disclosure) are satisfied.

Penalties

	MINIMUM PENALTY	MAXIMUM PENALTY
Violation because individual did not exercise ordinary care	$100 per violation with an annual maximum of $25,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
Violation due to reasonable cause but not willful neglect	$1,000 per violation with an annual maximum of $10,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
Violation due to willful neglect but is corrected within the allowed timeframe	$10,000 per violation with an annual maximum of $250,000 for repeat Violations	$50,000 per violation, with an annual maximum of $1.5 million
Violation due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

What should you do?

Fully-Insured Plans Only

Fully-insured group health, dental, and vision plans – employer does not receive any PHI from any of the plans (other than enrollment/disenrollment information).

Exempt from the privacy administration requirements.

Keep a copy of the plan privacy notices.

There is no such exemption in the Security rules.

Administrative Requirements

For employers with fully-Insured plans only and who do not receive any PHI other than enrollment and disenrollment information:

1. Designate a security official.
2. Establish a privacy policy prohibiting retaliation and waiver of rights.
3. Perform a risk analysis regarding any EPHI that the group health plan creates or receives (there should not be any EPHI received other than enrollment/ disenrollment information).
4. Adopt appropriate administrative, technical and physical safeguards for the EPHI (these requirements are scalable there should not be any ePHI received other than enrollment/disenrollment information).

Any Self-Insured Plan

Self-insured group plans; group health care, dental, vision, health FSAs, HRAs.

- First map the flow of information.
  - What information are you receiving from the health care plans?
  - Can you reduce the amount or type of PHI?
  - Why do you need PHI?
  - Who needs PHI?
  - Can the information be de-identified (removal of 18 identifiers)?
- Conduct an electronic security assessment.
- Implement the administrative requirements.

Note: a self-administered, self-insured plan with fewer than 50 participants is exempt from these requirements. Includes eligible employees and former employee.

Administrative Requirements

For employers that sponsor self-insured group health plans (medical, dental, vision, etc.):

1. Privacy official & Security Official
2. Perform a risk analysis regarding any ePHI that the group health plan creates or receives.
3. Policies & procedures
4. Designated contact person (may be privacy official)
5. Train employees
6. Establish a participant complaint process
7. Apply appropriate sanctions
8. Provide the Privacy Notice
9. Implement Business Associate Agreements

Plan Documents

Plan Documents:
The documents that create & maintain the plan

If the Employer wants PHI/EPHI the Plan Document must be amended to:

- Describe permitted uses and disclosures of PHI.
- Specify that disclosure is permitted only upon receipt of a certification from the plan sponsor that plan documents have been amended.
- Ensure that adequate firewalls are implemented.
- Any employee receiving PHI for administrative functions must be identified by name or function.
- Any disclosure to employees or classes of employees not identified in the plan documents is not a permissible disclosure.
- Implement administrative, physical, and technical safeguards.

The plan sponsor (employer) certifies that the plan document has been appropriately amended.

HRCI and SHRM Credits

- This Program, ID No. 537042, has been approved for 1.00 HR (General) recertification credit hours toward aPHR™, aPHRi™, PHR®, PHRca®, SPHR®, GPHR®, PHRi™ and SPHRi™recertification through HR Certification Institute® (HRCI®).

The use of this official seal confirms that this Activity has met HR Certification Institute's® (HRCI®) criteria for recertification credit pre-approval."

- Hays Companies is recognized by SHRM to offer Professional Development Credits (PDCs) for SHRM-CP® or SHRM-SCP®. This program is valid for 1 PDCs for the SHRM-CP or SHRM-SCP. Activity ID No. 20-X37GU. For more information about certification or recertification, please visit www.shrmcertification.org.

Thank you!

Hays
PART OF THE BROWN & BROWN TEAM

+

Brown & Brown INSURANCE