Brown & Brown

This Webinar Will Start Momentarily.
Thank you for joining us.

Brown & Brown

HIPAA Privacy & Security Overview

August 2022

Presented By:
Daniel Brady and Amanda Olimb

Presented by the Regulatory and Legislative Strategy Group

DISCLAIMER

Brown & Brown, Inc. and all its affiliates, do not provide legal, regulatory or tax guidance, or advice. If legal advice counsel or representation is needed, the services of a legal professional should be sought. The information in this document is intended to provide a general overview of the topics and services contained herein. Brown & Brown, Inc. and all its affiliates, make no representation or warranty as to the accuracy or completeness of the document and undertakes no obligation to update or revise the document based upon new information or future changes.

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 your 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

HIPAA Special Enrollments

Covered Entities:

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

Business Associates:

- Third-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 (e.g., dental plan, vision plan, health FSA, HRA, etc.)

The Regulated Information

Protected Health Information (PHI)

Health Information (HI)

Any information that—

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

+

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 – Privacy

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 Officer 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

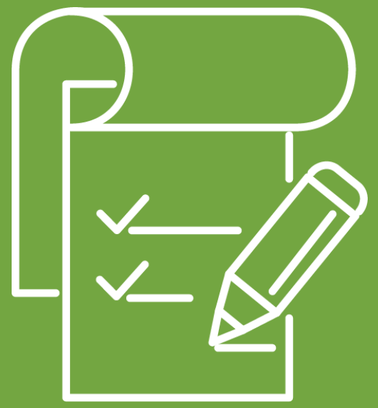
Secured PHI

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

Secured 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.

For breaches of unsecured PHI involving more than 500 residents of a State or jurisdiction, the media must be notified. HHS must also be notified immediately for breaches involving 500 or more individuals. For breaches involving fewer than 500 individuals, HHS must be notified, but not until after the year ends.

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 = Treatment, Payment, Health Care Operations

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.

Minimum necessary standard:

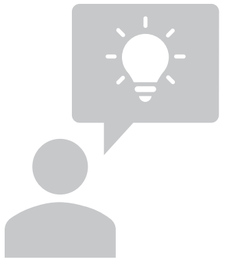
- Plan must make reasonable efforts to ensure that uses, disclosures or requests for PHI are limited to only the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

*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.

Authorization

- For uses and disclosers of PHI other than for treatment, payment, health care operations and certain other limited circumstances, the covered entity that has the PHI must obtain an authorization from the individual to whom the PHI pertains.

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



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

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 and 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).

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

Three Levels of Employer Records

Employees of the employer/ plan sponsor may:

- ✓ Receive summary health information for purposes of underwriting and settlor functions
- ✓ Receive any PHI for certain plan administration functions (i.e., health care operations) so long as the plan has been amended to allow such disclosures and the employer has established a firewall
- ✓ Enroll and disenroll participants and make payroll deductions
- ✓ Assist employees with understanding their plans

Employee/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 benefits 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)

Employee/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 from 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

Employee/Plan Sponsor

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	$127 per violation	$63,973 per violation, with an annual maximum of $1,919,173
Violation due to reasonable cause but not willful neglect	$1,280 per violation	$63,973 per violation, with an annual maximum of $1,919,173
Violation due to willful neglect but is corrected within the allowed timeframe	$12,794 per violation	$63,973 per violation, with an annual maximum of $1,919,173
Violation due to willful neglect and is not corrected	$63,973 per violation	$63,973 per violation, with an annual maximum of $1,919,173

Employer Considerations

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.

A plan’s hands-off status may be lost if employer’s broker/consultant receives PHI other than summary health information or enrollment/disenrollment information from an insurer on the plan's behalf.

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 officer

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 employees.

Administrative Requirements

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

1. Privacy Officer & Security Officer
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 Officer)
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

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. 601942,** 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®).

Brown & Brown 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. 22-WPZ62.** For more information about certification or recertification, please visit www.shrmcertification.org.

Brown & Brown

Find your solution at **BBrown.com**

DISCLAIMER: *Brown & Brown, Inc. and all its affiliates, do not provide legal, regulatory or tax guidance, or advice. If legal advice counsel or representation is needed, the services of a legal professional should be sought. The information in this document is intended to provide a general overview of the topics and services contained herein. Brown & Brown, Inc. and all its affiliates, make no representation or warranty as to the accuracy or completeness of the document and undertakes no obligation to update or revise the document based upon new information or future changes.*