Brown & Brown

HIPAA Privacy and Security Overview

August 2024

Presented By:
Christopher Bao and Cindy Niesen,
Brown & Brown 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.

Presentation Agenda

1. Covered Entities
2. Protected Health Information
3. HIPAA Privacy Overview
4. HIPAA Security Overview
5. Plan Sponsors and Employees
6. Summary

Covered Entities

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

Regulated Entities

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 healthcare plan is the covered entity (e.g., dental plan, vision plan, health FSA, HRA, etc.)

Health Plans

- Any individual or group plan that provides or pays the cost of healthcare
- **Exemption:** A self-insured health plan with fewer than 50 eligible employees is exempt if it is administered by the employer

EXAMPLES

- Medical plans (fully insured or self-insured)
- Employee Assistance Plans (that provide medical care)
- Dental and vision plans
- Prescription drug plans
- Health reimbursement arrangements (HRAs)
- Health flexible spending arrangements (FSAs)
- Wellness programs that provide medical care

Protected Health Information (PHI)

Regulated Information

Protected Health Information (PHI)

Health Information (HI)

Any information that—

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

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

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)

HIPAA Privacy Overview

Basic Requirement – Privacy

Three primary protections:

Use and Disclosure Rules	Limit when covered entity can use or disclose individual's PHI. In general, cannot use or disclose unless permitted by Privacy Rule or authorized by individual
Individual Rights	Provide individuals with certain rights with respect to their PHI, including right to receive a Privacy Notice
Administrative Safeguards	Require covered entities to develop written privacy procedures and implement appropriate safeguards, including designating a privacy officer and training employees

Use and Disclosure Rules

TPO = Treatment, Payment, Health Care Operations

PHI may be used or disclosed within the TPO universe without authorization

Inside the TPO Universe

- Treatment by healthcare provider
- Payments by health plans
- 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

Other non-TPO Uses/Disclosures include:

- Disclosures to family members
- Disclosures for specific public policy purposes (e.g., when required by law, for public health activities, for judicial and administrative proceedings, etc.)

Use and Disclosure Rules

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

Plan Sponsors & PHI

Covered entity may disclose the following PHI to the plan sponsor:

- Plan enrollment information
- Summary health information (to obtain premium bids or modify or terminate the plan)
- PHI of group health plan enrollees for plan administration purposes
  - » 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

Plan Documents

If the plan sponsor wants PHI/ePHI, the Plan Document must be amended to:

- Describe permitted uses and disclosures of PHI
- Incorporate provisions specifying that the group health plan will disclose PHI to the plan sponsor only upon receipt of a certification from the plan sponsor that plan documents have been amended. Plan sponsor must agree to:
  - » Not use or further disclose the information, other than as permitted or required by the plan documents or as required by law;
  - » Ensure that any agents to whom PHI is provided agree to the same restrictions and conditions;
  - » Not use or disclose for employment-related actions and decisions;
  - » Report to the group health plan any uses or disclosures that are inconsistent with the permitted uses or disclosures of which it becomes aware;
  - » Make PHI and internal practices, books and records to HHS to determine compliance;
  - » Make PHI available for amendment or to provide for an accounting of disclosures

Administrative Standards

The Covered Entity must:

Adopt a privacy policy and administrative procedures

Comply with plan document provisions

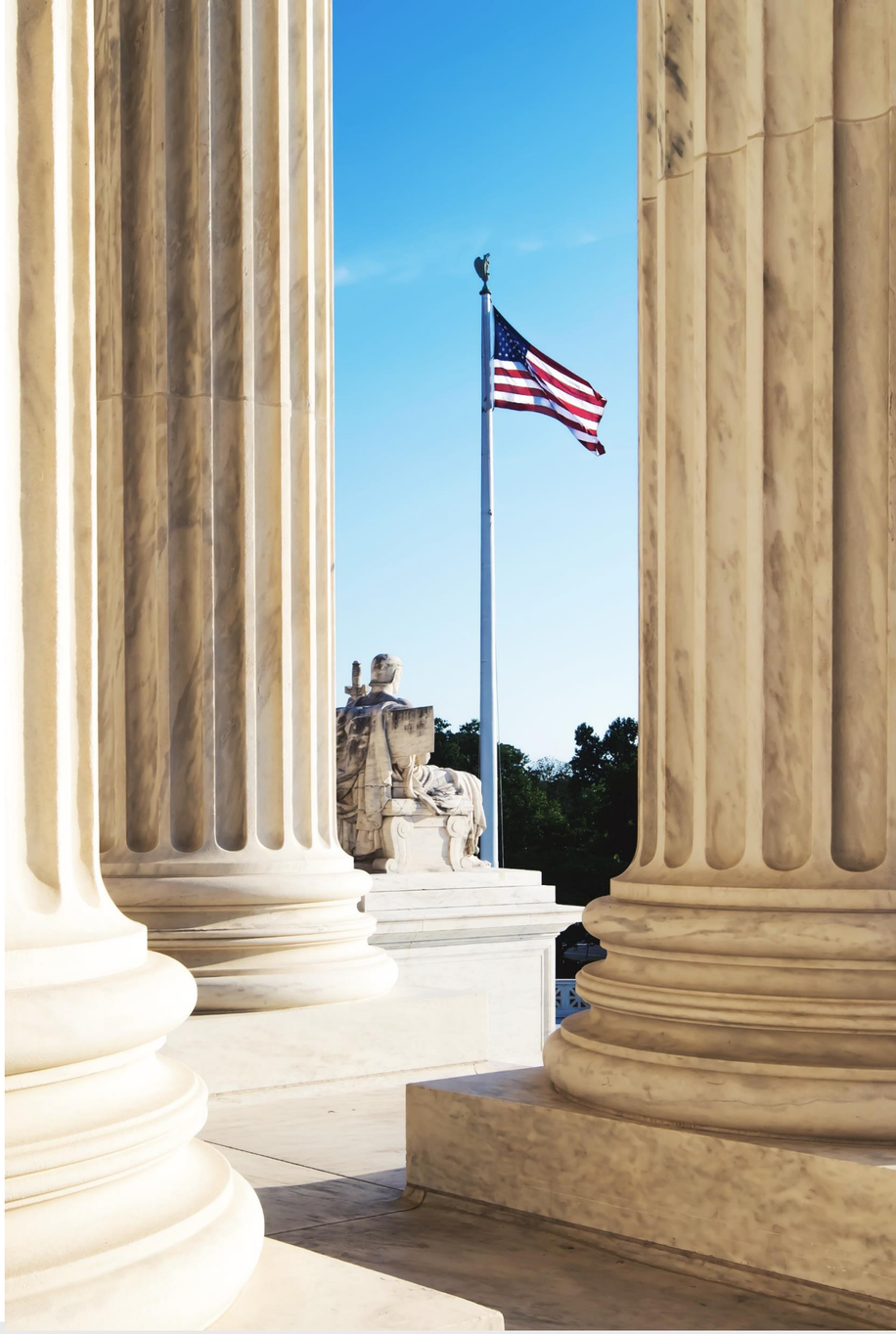
Implement organizational, physical and technical safeguards and adequate firewalls

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

Note: Any disclosure to employees or classes of employees not identified in the plan documents is not a permissible disclosure

Administrative Requirements

1. Privacy Officer & Security Officer
2. Adopt policies & procedures
3. Designated contact person (may be Privacy Officer)
4. Train employees
5. Establish a participant complaint process
6. Apply appropriate sanctions
7. Implement Business Associate Agreements



Use or Disclosure Pursuant to Authorization

For uses and disclosures of PHI other than for treatment, payment, healthcare 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.

Other Permitted Uses and Disclosures

PHI can be shared by the covered entity without specific consent for the following purposes:

- To address public health and safety issues (e.g., disease prevention, product recalls, reporting adverse medication reactions or reporting suspected abuse, neglect or domestic violence)
- For health oversight activities authorized by law
- For health research
- To regulatory agencies to comply with state or federal laws
- To organ procurement organizations to respond to organ and tissue donation requests
- To work with a medical examiner or funeral director
- For workers' compensation claims
- For law enforcement purposes and special government functions (e.g., military, national security and presidential protective services) and
- In response to a court or administrative order or subpoena

Individual Rights

Include:

Right of access

Right to amend/ correct PHI

Right to obtain accounting of disclosures

Right to receive notice of privacy practices

Right to request restrictions on uses and disclosures

Right to request alternative communications

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 (However, the group health plan is responsible for compliance and is required to maintain a Privacy Notice if the plan sponsor or a business associate receives PHI, and to provide the notice upon request)
- If self-insured – Plan responsibility

Notice must be sufficiently detailed to inform individual of privacy practices

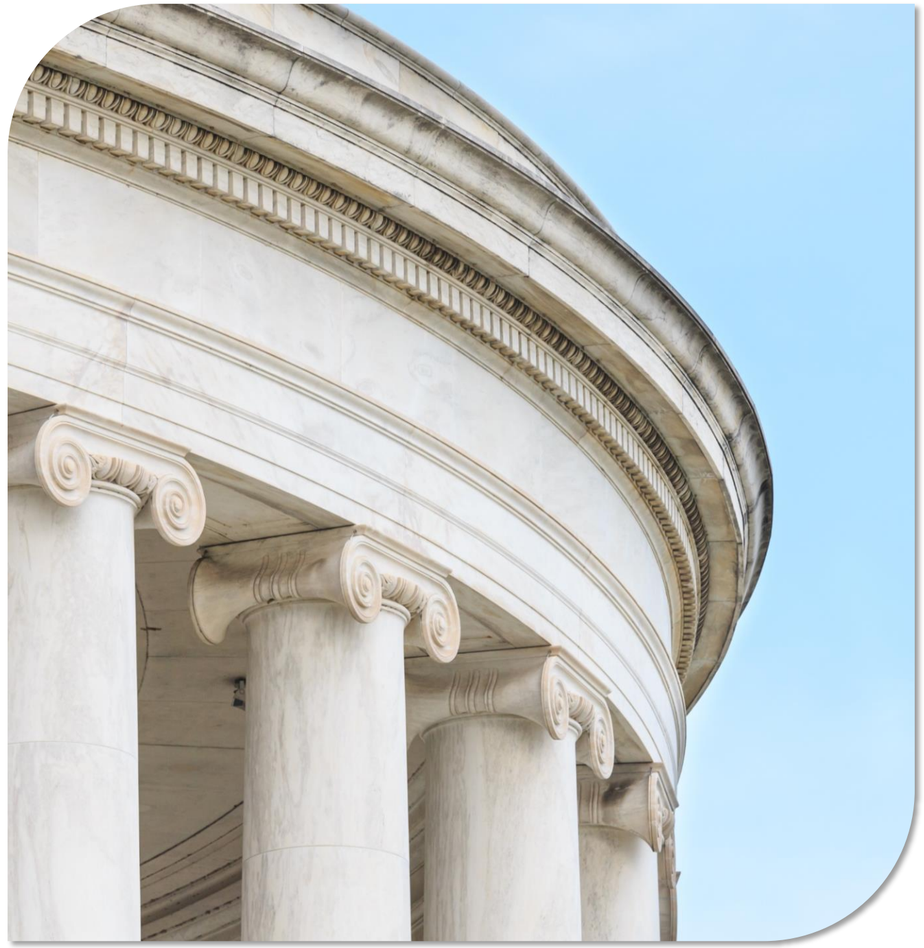
Privacy Notice Requirements

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



HIPAA Security Overview

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 must perform a risk analysis regarding any ePHI that the group health plan creates or receives. Policies and procedures dictated by results of risk analysis

Security Requirements

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

Security Requirements

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

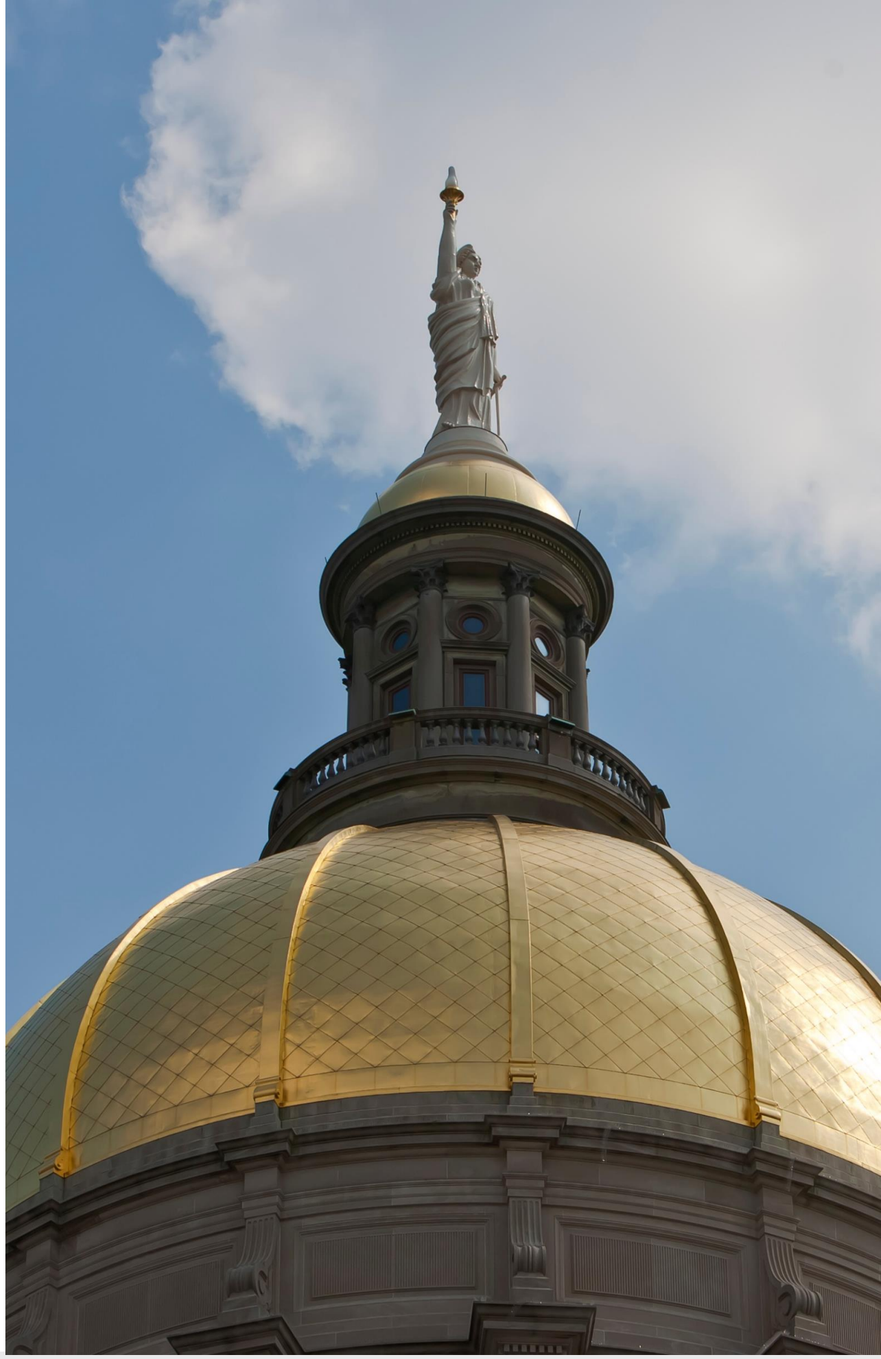
For breaches of unsecured PHI involving more than 500 residents of a State or jurisdiction, the media must be notified. HHS must also be notified immediately for breaches involving 500 or more individuals. For breaches involving fewer than 500 individuals, HHS must be notified, but not until after the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

Plan Sponsors and Employers

Business Associates and PHI

Covered entity may disclose PHI to Business Associate for TPO purposes.

- A written business associate agreement must be in place
- Agreement must establish permitted and required uses and disclosures of PHI by business associate
- Business associate must protect PHI
- Business associate cannot use or disclose PHI in a manner that would violate the HIPAA rules



Three Levels of Employer Records

Individually Identifiable Information

Level 3	Medical information from group health plan or healthcare 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 HIPAA Responsibilities

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 Access to Information

Employees of the employer may:

- ✓ Receive summary health information for purposes of underwriting and settlor functions
- ✓ Enroll and disenroll participants and make payroll deductions
- ✓ Assist employees with understanding their plans

Prohibited Actions

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, Disability claims, Health Savings Account, Dependent Care Assistance Plans and other programs

- The insurance carrier or HSA custodian is not a covered entity
- May be subject to other privacy laws, such as Gramm-Leach-Bliley Act (GLBA) which applies to financial services industry and/or state employment laws

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

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, healthcare 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

Final Rules on Reproductive Health Rights

Final Rule: HIPAA to Apply to Reproductive Healthcare PHI

Law:

- On April 26, 2024, the Office for Civil Rights (OCR) at the U.S. Department of Health & Human Services (HHS) published its Final Rule to Support Reproductive Health Care Privacy.

- According to OCR, the goal when adopting these rules is to create a “purpose-based prohibition” on specific uses and disclosures of Protected Health Information (PHI) related to the reproductive health of individuals.

- **If the RH service is <u>legally</u> obtained, a health plan cannot disclose <u>reproductive health</u> PHI to law enforcement or someone seeking to sue the participant/healthcare provider.**

Health Plans as Covered Entities under HIPAA

- Health Plans are considered Covered Entities under HIPAA and subject to the Privacy and Security Rules, unless an exception applies. Most health plans will be required to have a Policies and Procedures, Business Associate Agreements with Business Associates, Authorizations for release of PHI and a Notice of Privacy Practices that is disclosed to plan participants.

- Health Plans/Employers should discuss with their legal counsel whether and how to update their HIPAA Policies and Procedures, BAAs and their Notice of Privacy Practices.

Reproductive Healthcare PHI Protections Do Not Apply to the Following Situations

Exceptions to the Final Rule

- When a healthcare provider uses/discloses PHI to help defend itself against an investigation related to professional misconduct or negligence involving reproductive healthcare
- A covered entity using/disclosing PHI to help defend anyone involved in a criminal, civil or administrative proceeding where liability could exist in providing reproductive healthcare
- A covered entity or a related business associate uses/discloses PHI to a Statutory Inspector General that seeks to conduct an audit for health oversight purposes
- **Attestation must be provided to covered entity from requester, to attest that information will not be used for a prohibited purpose**

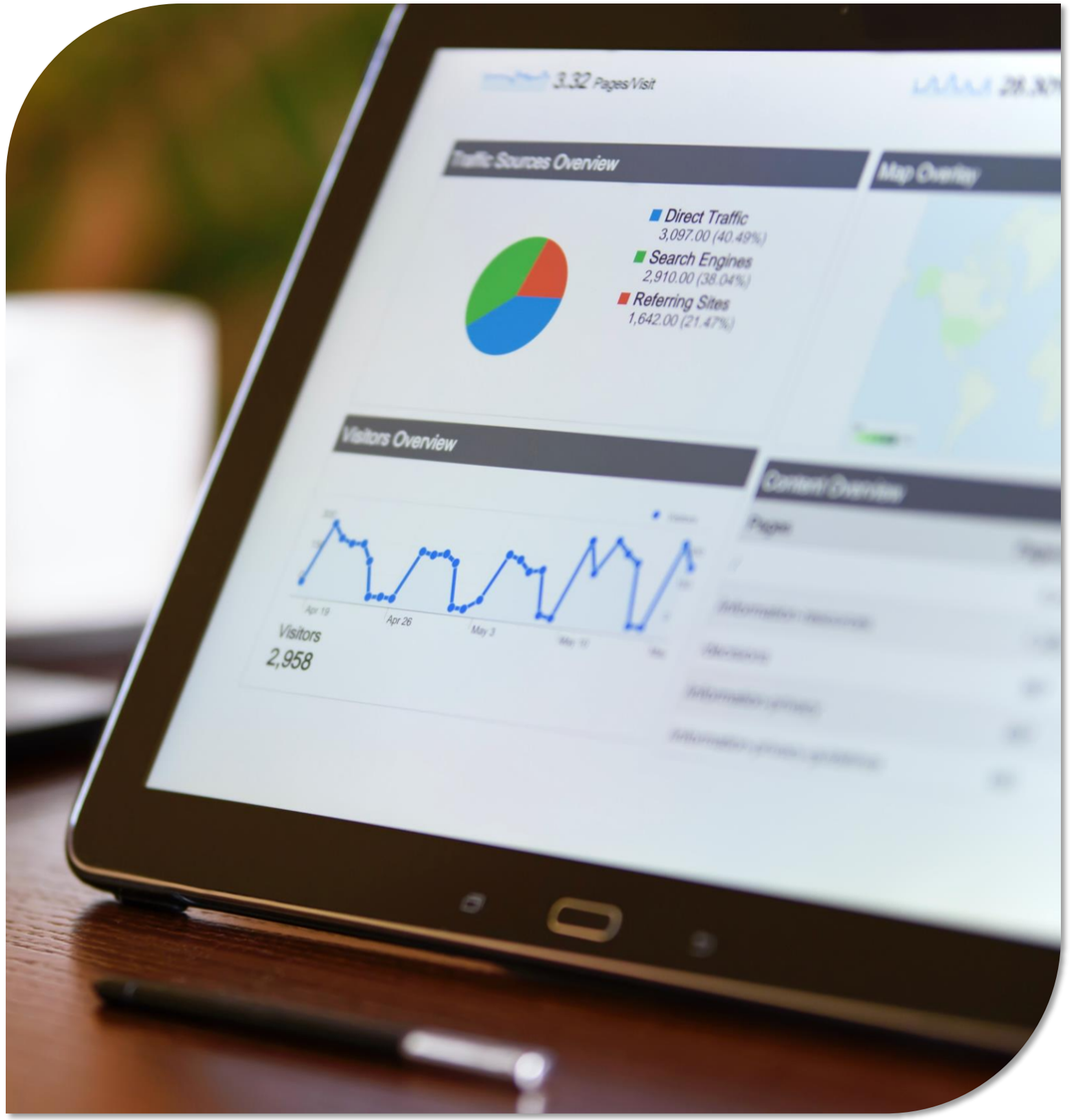
Next Steps

ACTION PLAN

The following are considerations when discussing issues related to reproductive healthcare:

- Customers should review their current HIPAA Policies and Procedures and BAAs and update them as necessary by December 23, 2024.

- Customers should update their Notice of Privacy Practices by February 16, 2026.



Summary

Key Takeaways

- Access, use or provide only the Minimum Necessary PHI to accomplish the task
- Cover, turn over or lock up PHI that is not immediately in use
- Report accidental or willful disclosures of PHI to your HIPAA Privacy Officer or Supervisor
- Do not discuss PHI outside of work environment under any circumstances
- Never leave open files and documents containing PHI unattended

- Always dispose of PHI according to current Policies and Procedures
- When you must discuss PHI, lower your voice or move to a private area
- Protect PHI on computers, cell phones, fax machines and other electronic devices.
- Best practice: use encryption for email containing PHI
- Always file, shred, secure or otherwise properly dispose of PHI
- If in doubt about what to do, ask your Supervisor or HIPAA Privacy Officer

Civil Penalties (inflation-adjusted as of 8/8/2024)

	MINIMUM PENALTY	MAXIMUM PENALTY
Violation because individual did not exercise ordinary care	$141 per violation	$71,162 per violation, with an annual maximum of $2,134,831
Violation due to reasonable cause but not willful neglect	$1,424 per violation	$71,162 per violation, with an annual maximum of $2,134,831
Violation due to willful neglect but is corrected within the allowed timeframe	$14,232 per violation	$71,162 per violation, with an annual maximum of $2,134,831
Violation due to willful neglect and is not corrected	$71,162 per violation	$71,162 per violation, with an annual maximum of $2,134,831

In addition to civil penalties, criminal penalties can be imposed for intentional violations.

HRCI and SHRM Credits

This Program, **ID No. 668911** ,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. 24-9HSMW**. 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.*

© 2024 Brown & Brown. All rights reserved.