Wespath
BENEFITS | INVESTMENTS

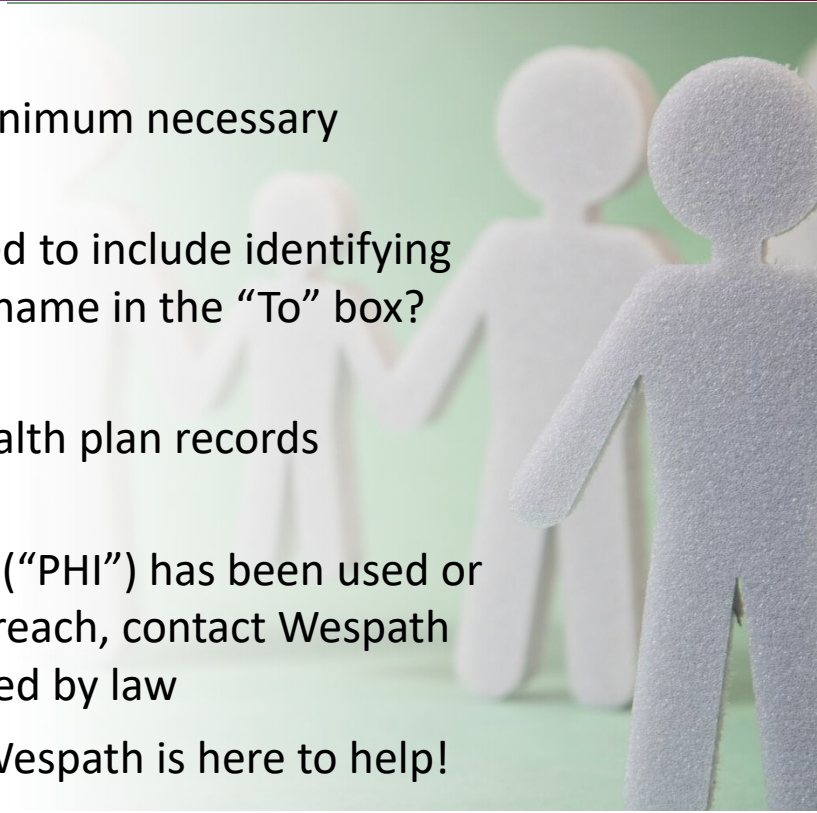
HIPAA Privacy & Security Training for Plan Sponsors

Topics

- Key Terminology & Concepts
- Uses and Disclosures of PHI
- Individual Rights of Participants
- Safeguards for Protecting PHI
- Consequences of Violations
- Examples

Top 5 Training Take-Aways

1. **Use the minimum!**
   If you need to use or disclose PHI, choose the minimum necessary
2. **Slow down!**
   Be mindful when emailing PHI: Do you really need to include identifying information? Is the correct/intended recipient's name in the "To" box?
3. **Keep it separate!**
   Do not commingle records with PHI with non-health plan records
4. **Act quickly!**
   If you suspect that protected health information ("PHI") has been used or disclosed improperly or has been involved in a breach, contact Wespath as soon as possible -- quick action may be required by law
5. **Ask us!** If you are ever unsure about using PHI, Wespath is here to help!



Key Terminology & Concepts

What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)
- Purposes of HIPAA
  - To provide greater access to health care insurance (i.e., special enrollment and nondiscrimination rules)
  - To promote standardization and efficiency in the health care industry (i.e., coding for health care transactions)
  - ***To protect the privacy of health care information (i.e., privacy and security rules)***

HIPAA Privacy & Security Rules

- The HIPAA privacy and security rules protect individually identifiable health information
  - Privacy Rule:
    - Sets rules for how protected health information ("PHI") may be used and disclosed
    - Gives participants certain rights regarding their PHI
    - Requires notification to impacted participants and others in the event of certain breaches
  - Security Rule: Requires a covered entity to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting electronic PHI ("E-PHI")

HIPAA privacy and security rules are enforced by the U.S. Department of Health & Human Services ("HHS")

What is the HIPAA covered entity?

- A group health plan is a “covered entity” under HIPAA, which means it is subject to HIPAA’s privacy and security rules
  - HealthFlex and the Medicare Marketplace & HRA Program (Via Benefits) (each, a “Plan” and collectively, the “Plans”) are covered entities under HIPAA
  - HealthFlex is considered a “hybrid entity” under HIPAA because it has group health plan benefits and non-health plan benefits
    - HealthFlex’s covered entity components include only the group health care benefits, including the medical and behavioral health plans, vision and dental benefits, health care FSA and HRA and well-being programs (the dependent care FSA program and HSA are *not* part of the covered entity)
- All plan sponsors have signed a HIPAA certification form acknowledging HIPAA’s requirements

Key Parties

- A covered entity acts through its HIPAA “workforce”
  - Workforce members include all individuals at Wespath and at the plan sponsors who may have access to PHI in connection with administration of the Plans
  - The Plans maintain a HIPAA Policy Manual to guide the Plans’ workforce in HIPAA compliance (the Manual is primarily intended for plan administration activities by Wespath staff)

Key Parties *(continued)*

- HIPAA requires designation of a HIPAA Privacy Officer:
  Stacy Amato, Manager – Compliance at Wespath
- HIPAA "business associates" are outside individuals or entities that create, receive, maintain, or transmit PHI for a covered entity
  - Business associates are obligated by law to comply with HIPAA and must sign a detailed contract ("business associate agreement") with the covered entity outlining its obligations
  - Examples: BCBSIL, UHC, Cigna, VSP, OptumRx, Quest Diagnostics

You are part of the HIPAA workforce if you have access to PHI in connection with Plan administration; plan sponsors have very limited access to PHI, so have a very limited "workforce" role

What is Protected Health Information ("PHI")?

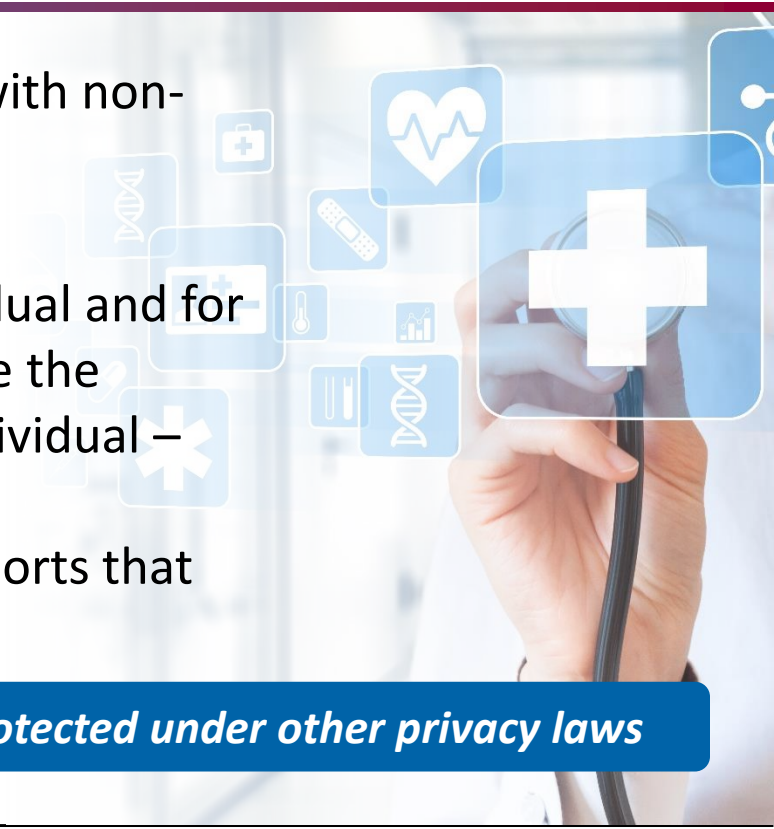
- PHI is information that is created, maintained, or received by a covered entity or business associate that:
  - identifies an individual (or contains enough information to reasonably identify the individual) and
  - relates to the past, present, or future health or condition of an individual, the provision of health care to an individual, or payment for the provision of health care to an individual
- Includes demographic information when tied to the Plan
- Can be maintained in any form (i.e., electronic, hard copy, oral)
- Examples of items that might contain PHI plan sponsors receive from Wespath: invoices, census lists, well-being program completion lists

What is not PHI under HIPAA?

- Plan enrollment information (including premium amounts) in the hands of plan sponsors *acting as the employer*
  - HIPAA requires “adequate separation” between plan sponsors acting as the employer and the Plans
- Health information in employment records held by plan sponsors acting as the employer
  - **Do not commingle employment records with records of the Plans (use a “firewall”)**

What is not PHI under HIPAA? *(continued)*

- Health information received in connection with non-health plan benefits (e.g., related to CPP or UMLifeOptions)
- Information that does not identify an individual and for which there is no reasonable basis to believe the information could be used to identify an individual – "de-identified health information"
  (e.g., the quarterly and annual summary reports that Wespath provides to plan sponsors)



But keep in mind that this information may be protected under other privacy laws

What PHI might plan sponsors receive?

- Examples of items that might contain PHI plan sponsors receive from Wespath: invoice detail, census lists, well-being program completion lists
- Quarterly reports and annual summary reports that Wespath provides to plan sponsors generally do not contain PHI because they do not include individually identifiable information

Uses & Disclosures of PHI

Uses & Disclosures: The General Rule under HIPAA

- Workforce members of the Plans may use and disclose PHI for treatment, payment, and health plan operations without obtaining a participant's written authorization
- Otherwise, to use or disclose PHI, a workforce member must:
  - have a signed authorization from the participant, *or*
  - satisfy one of HIPAA's exceptions
- In all cases, the "minimum necessary standard" applies -- only the minimum necessary PHI may be used or disclosed for the intended purpose
- Workforce members must use adequate safeguards to protect oral, hard copy, and electronic PHI

Uses & Disclosures: Treatment, Payment, or Health Plan Operations

- ***Treatment*:** Providing, coordinating, or managing health care and related services by health care providers
- ***Payment:*** Activities to obtain premiums, obtain or provide reimbursement for the provision of health care, or determine the Plan's responsibility for coverage
- ***Health Plan Operations:*** General plan administration, quality assessments, evaluation of coverage, and case management

Uses & Disclosures: Participant Authorization

- A written authorization is needed for disclosures that are not for treatment, payment, or health plan operations and do not satisfy one of HIPAA's exceptions (e.g., a participant wants us to share info with a lawyer who is helping appeal a claim denial)
- To be valid, an authorization must contain very specific information
  - If you receive an authorization from a participant or third party, ask the Privacy Officer at Wespath to review it to confirm it includes all required information
- An authorization can be revoked by written notice

Uses & Disclosures: Individuals Identified by the Participant

- Disclosures may be made to a spouse, relative, friend, or other individual identified by a participant as follows:
  - If the participant is present, you must obtain the participant's agreement unless you can reasonably infer from the circumstances that the participant does not object to the disclosure
  - If the participant is not present *and* the participant's agreement cannot practicably be provided because of incapacity or emergency, you may determine whether the disclosure is in the best interests of the participant and if so, disclose PHI that is directly relevant to the other individual's involvement with the participant's care or payment for the participant's care

Uses & Disclosures: Personal Representatives

- A participant may designate another individual to be his or her "personal representative"
- A participant's personal representative has all the rights of the participant with respect to disclosures of PHI
- Contact Wespath's HIPAA Privacy Officer *before* disclosing PHI to anyone claiming to be a personal representative of a participant
  - The Privacy Officer will confirm that the individual has met all requirements to be a personal representative

Keep in mind: Personal representatives only have rights with respect to PHI under HIPAA; if the personal representative is going to take action on behalf of the participant (e.g., make a benefit election) a power of attorney, guardianship, or other documentation may be required

Uses & Disclosures: Disclosure of a Minor's PHI to a Parent

- A parent is automatically the personal representative of his or her *minor* child
- You can disclose the PHI of a minor child to his or her parent unless:
  - the disclosure is inconsistent with state law;
  - the minor is the one who consents to care and the consent of the parent is not required under state or other applicable law;
  - the minor obtains care at the direction of a court or person appointed by a court; or
  - the parent agrees that the minor and the health care provider involved may have a confidential relationship
- A parent is not automatically the personal representative of his or her *adult* child

Uses & Disclosures: Participant's Disclosures to the Plan Sponsor

- If a participant discloses his/her PHI (or a dependent's PHI) to the plan sponsor to seek the plan sponsor's assistance with respect to a claim, the plan sponsor can use and disclose the PHI to communicate with Wespath with respect to the claim
- However, the minimum necessary standard always applies
- Also, appropriate safeguards should be used, e.g.:
  - Consider whether it is necessary to retain any hard and electronic copies and properly dispose of them to the extent it is not necessary
  - If you think additional protections are appropriate when sending the PHI by email, reach out to Wespath to discuss other secure messaging (Zix)

Uses & Disclosures: Other Exceptions

HIPAA provides exceptions for certain uses and disclosures:

- Required by law
- Related to government functions (e.g., public health, law enforcement)
- Related to lawsuits and disputes
- To prevent or lessen a serious and imminent threat to the health or safety of you, another person, or the public

Uses & Disclosures: Other Exceptions *(continued)*

- To a coroner, medical examiner, or funeral director as necessary to carry out their duties
- A workforce member may disclose PHI to a workers' compensation insurer or other employee at the plan sponsor who administers workers' compensation benefits, but only:
  - as necessary to comply with workers' compensation laws, or
  - for purposes of obtaining payment for any health care provided to the injured employee

Individual Rights of Participants

Individual Rights Provided by HIPAA

- ***Access to PHI:*** right to access and copy most PHI that is part of Plan records
- ***Amendment of PHI:*** right to amend most PHI that is created by or on behalf of the Plan
- ***Accounting of Disclosures of PHI:*** right to a list of certain disclosures of PHI made by the Plan for the previous 6 years
- ***Confidential Communications of PHI:*** right to receive communications of PHI by other means or at a different location if the normal method could endanger the participant
- ***Restriction on the Use and Disclosure of PHI:*** right to request restrictions on the use and disclosure of the participant's PHI
- ***Privacy Notice:*** right to notice of the Plan's privacy practices at enrollment, upon request, and after a material change (and notice of its availability at least once every three years)

Individual Rights *(continued)*

- These rights are not absolute – there are limitations
- Wespath and plan sponsors are prohibited from intimidating, threatening, coercing, discriminating against, or taking any retaliatory action against a participant for exercising his or her rights under HIPAA
- If you are contacted by a participant who wants to exercise one of these rights, contact the Wespath Health Team

Safeguards for Protecting PHI

Safeguards for Oral & Hard Copy PHI

- Only discuss PHI in your office or another room with the door closed
- PHI should not be left out and unattended on your desk or at a printer
- Dispose of material containing PHI in secure trash bins, ideally shredded
- Lock offices and file cabinets containing PHI
- Avoid leaving PHI in an unattended car or in checked luggage

Remember – the minimum necessary standard always applies

Safeguards for Electronic PHI

- When transmitting E-PHI to Wespath or a third-party business associate, use a secure website or Zix instead of email when appropriate and feasible
  - You can request/respond to a Zix email initiated by Wespath with particularly sensitive PHI
- Use password protection and encryption whenever possible
- If you must use email to transmit E-PHI:
  - Eliminate identifiers to the extent possible
  - Use caution regarding recipients (triple check recipient names)

Safeguards for Electronic PHI *(continued)*

- Avoid storing your laptop or phone in an unattended car or in checked luggage
- Log off from your computer when you leave your workstation
- Keep your computer screen out of sight from others
- Never download E-PHI to your personal computer or send it to your personal email address
- Consider applicable retention policies and needs – if you no longer need an email or document with E-PHI, double delete it

Remember – the minimum necessary standard always applies

Consequences of HIPAA Violations

General Breach Notification Rule

- Any acquisition, use, or disclosure of “unsecured” PHI that is not allowed by HIPAA is considered a breach unless an exception applies
  - PHI is secured if it is rendered unusable or unreadable by unauthorized individuals through encryption or destruction
  - Very limited exceptions (e.g., inadvertent disclosure of PHI to another authorized HIPAA workforce member; inability of the recipient to retain any PHI)
- If there is a breach of unsecured PHI, the Plan must provide notice of the breach to impacted participants, the Department of Health and Human Services (HHS), and in certain circumstances, the media

Timing of Breach Notification

- Notification must be made without unreasonable delay and no more than 60 days from "discovery" of the breach
  - A breach is considered "discovered" as of the first day that it is known (or reasonably should have been known) to the Plan
  - The Plan has knowledge of the breach on the day that *any* HIPAA workforce member or other agent has such knowledge
  - *This means it is critically important that you report to the Wespath HIPAA Privacy Officer as soon as you **suspect** a breach may have occurred – the Plan's time to respond starts ticking at the time **you** discover the breach*
  - The Privacy Officer will complete a breach investigation report and determine whether notice is required

Sanctions for HIPAA Violations

- Civil Penalties
  - Tiered system depending on the level of culpability ranging from $100 to $50,000 per violation; maximum of $1,500,000 per year for multiple violations of the same part of HIPAA
  - Each day a violation continues can be counted as a separate violation
- Criminal Penalties
  - Up to $50,000 fine plus one-year imprisonment for knowingly violating HIPAA
  - Up to $100,000 fine plus five years' imprisonment for falsifying PHI
  - Up to $250,000 fine plus ten years' imprisonment for violating HIPAA with the intent to profit or do harm

Examples of Actual Penalties & Settlements

- CVS paid $2.25 million to settle allegations that it disposed of sensitive customer prescription information in easily accessible dumpsters
- Affinity Health Plan paid $1.2 million to settle an investigation into its alleged failure to erase PHI from a leased photocopier upon returning it
- Massachusetts General Hospital paid a $1 million penalty after an employee lost the medical records of 192 patients on a subway train
- Blue Cross Blue Shield of Tennessee paid $1.5 million to settle an investigation into its alleged failure to properly re-evaluate security measures in response to a theft of hard drives containing PHI
- Lifespan Health System paid $1 million to settle alleged violations related to the theft of a hospital employee's unencrypted laptop that contained patient PHI

Other Consequences of HIPAA Violations

- Damage to Wespath's and the plan sponsor's reputations
- Increased likelihood of future audits by HHS
- HIPAA requires the plan sponsor to appropriately discipline any employee who violates HIPAA

Example 1: The Concerned Plan Sponsor

- Facts: As a plan sponsor benefits office representative, you are a member of HealthFlex's HIPAA workforce. Marcel is Remy's supervisor in the benefits office. Remy has been calling in sick for work a lot recently. Marcel calls you and asks "Do you know if Remy is actually sick? Can you ask Wespath if he has claims?"
- Can you gather or share any information with Marcel? No. A disclosure of PHI in this situation is not a permitted purpose under HIPAA.
- What if Marcel is asking to confirm information Remy submitted for an FMLA leave request? No. There is no exception under HIPAA with respect to FMLA.

Example 2: The Party Planner

- Facts: As a plan sponsor benefits office representative, you are a member of HealthFlex's HIPAA workforce. A coworker, Sam, is planning a party for clergy and is trying to estimate how many clergy will bring a spouse. He asks you if Joe covers a spouse under the health plan.
- Can you share this information with Sam? No. The mere fact that someone is covered by the health plan is considered PHI. Sharing this information with Sam would be an impermissible disclosure of PHI.

Example 3: The Curious Consultant

- Facts: As a plan sponsor benefits office representative, you are a member of HealthFlex's HIPAA workforce. Your consultant (a HIPAA business associate with a valid business associate agreement) would like a more detailed list of high-cost claimants and their conditions from HealthFlex to discuss with the insurance committee. You request more detailed information from Wespath.
  - Is this a HIPAA violation? Maybe not. Depending on the nature of the high-cost claims, it may be possible to identify individuals even if that detail isn't provided. Wespath will encourage you and your consultant to make sure that the request meets the minimum necessary standard, will be used for a permitted reason, and will ensure the individual receiving the data has a signed HIPAA Certification form. Wespath may group the high-cost claimants into categories rather than listing as individuals, for example.
- What if your consultant *isn't* a HIPAA business associate with a valid business associate agreement?
  - PHI cannot be shared with the consultant under any circumstances. You should discuss this request with Wespath and consider approaches to de-identify the information.

Example 4: Minimum Necessary for Requests

- Facts: You need to know how many participants elected to contribute to a health care FSA. You request their name, SSN, p#, DOB, and FSA enrollment and amount elected.
- Has the request met the minimum necessary standard? No. If you only need to know the number of participants enrolled in the FSA, the request does not comply with the minimum necessary standard. To comply with this standard, the request could be for name and enrollment only.

Wespath

BENEFITS | INVESTMENTS