NEWFRONT

HIPAA Training for Employers

2026 Edition

Audio

Presented by: **Brian Gilmore | Lead Benefits Counsel, VP**

Guide Topics

HIPAA Training for Employers

From Portability to Privacy and Security

- HIPAA = The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Two main branches of HIPAA compliance—Portability and Privacy (most trainings cover only Privacy)
- This session will cover both aspects of HIPAA, with a focus on the Privacy training component
- HIPAA imposes the only mandatory employee benefits-related training requirements for employers with self-insured plans
- Use this session to satisfy and document your training requirement if you are within the HIPAA firewall!

HIPAA Portability and Privacy Topics for Discussion

1. **Portability:** HIPAA special enrollment events, ACA eliminates certificates of creditable coverage
2. **Nondiscrimination:** HIPAA and ACA's extensive structure of rules to regulate wellness programs
3. **Covered Entities:** All employer-sponsored group health plans are HIPAA covered entities
4. **PHI:** What qualifies as Protected Health Information, the big exception for enrollment data, and case studies of enforcement
5. **Compliance Strategies:** How to avoid a HIPAA breach and satisfy documentation requirements

Don’t Forget: Document Training

Template employee HIPAA training sign-in sheet

Click here for a fillable pdf employee sign in sheet you can use!

NEWFRONT

Employee HIPAA Training Sign-In Sheet

Topic: HIPAA Privacy and Security Training

Presenter: Brian Gilmore, Newfront Lead Benefits Counsel

Date: **Time:**

	Employee Name	Employee Signature
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

HIPAA – The Big Picture

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)

HIPAA includes two main areas for employers.

HIPAA Portability

Pre-ACA (Eliminated in 2014)

- Pre-Existing Condition Exclusion (PCE) Limitations
- Notices of Creditable Coverage

Still in Effect

- Special Enrollment Events
  - Required Mid-Year Enrollment Events
- Nondiscrimination Based on Health Status
  - Primary Application is to Wellness Programs

HIPAA Privacy and Security
(Technical Name: Administrative Simplification)

HIPAA Privacy (Added 2003)

- Covered Entity
- Protected Health Information
- Business Associates and BAAs
- Minimum Necessary Rule
- Breach of Unsecured PHI Notifications (HITECH Act)
- Strategies and Situations

HIPAA Security (Added 2005)

- Administrative, Physical, and Technical Safeguards


HIPAA
Portability

01

Pre-ACA Requirements

Certificates of Creditable Coverage

ACA PCE Prohibition

Ended HIPAA Certificates of Creditable Coverage

As of December 31, 2014, health plans are no longer required to provide a HIPAA certificate of creditable coverage upon the loss of coverage.

- Reason is that ACA now prohibits health plans from imposing any pre-existing condition exclusions
- Therefore, individuals will no longer need to provide evidence that they have maintained creditable coverage to avoid pre-existing condition exclusions

There is no uniform type of documentation plans rely on to substantiate a mid-year HIPAA special enrollment event based on loss of other coverage.

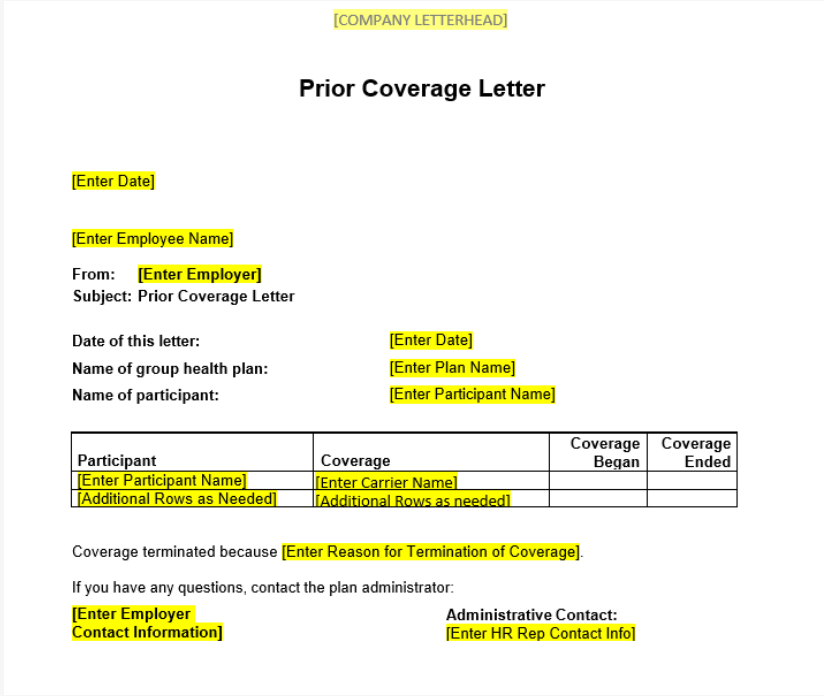
- In the past, plans and carriers typically relied on the HIPAA certificate of creditable coverage as evidence of the mid-year loss of coverage
- **Best alternative is the employer providing a letter on its letterhead stating when coverage under the plan terminated (but this should no longer be a HIPAA certificate with obsolete rights listed)**

- Other possible alternatives (from the old pre-2015 regulations, but still useful) include:
  - EOBs or other correspondence from plan or issuer indicating coverage
  - Pay stubs showing payroll deductions for health coverage
  - Third-party statements verifying periods of coverage (e.g., from employer)
  - Phone call from plan or provider to third-party verifying coverage
  - Health ID cards
  - Records from medical providers indicating coverage

Life After HIPAA Certificates

Documenting Prior Coverage

Preferred alternative to the obsolete HIPAA certificate of creditable coverage to substantiate a mid-year HIPAA special enrollment event based on loss of other coverage.



[COMPANY LETTERHEAD]

Prior Coverage Letter

[Enter Date]

[Enter Employee Name]

From: **[Enter Employer]**
Subject: Prior Coverage Letter

Date of this letter: [Enter Date]
Name of group health plan: [Enter Plan Name]
Name of participant: [Enter Participant Name]

Participant	Coverage	Coverage Began	Coverage Ended
[Enter Participant Name]	[Enter Carrier Name]		
[Additional Rows as Needed]	[Additional Rows as needed]		

Coverage terminated because [Enter Reason for Termination of Coverage].

If you have any questions, contact the plan administrator:

[Enter Employer Contact Information]

Administrative Contact:
[Enter HR Rep Contact Info]

02

Special Enrollment Events

Mid-Year Health Plan Enrollment Rights

HIPAA Special Enrollment Events

Which Events Qualify?

The following events qualify as HIPAA special enrollment events:

- Loss of eligibility for other group health coverage or individual insurance coverage
- Loss of Medicaid/CHIP eligibility or becoming eligible for a state premium assistance subsidy under Medicaid/CHIP
- Acquisition of a new spouse or dependent by marriage, birth, adoption, or placement for adoption

The medical plan **must** permit employees to make election changes as required by HIPAA

- Other Section 125 permitted election change events are optional for employer and carrier/stop-loss to recognize
- The medical plan and insurance carrier/stop-loss must accommodate all HIPAA special enrollment events

Right to Change Medical Plan Options

- Upon experiencing a HIPAA special enrollment event, the plan is required to allow the employee to select any medical benefit package under the plan
  - For example, move from Kaiser to UHC, Cigna to Kaiser, HMO Low to PPO High, etc.

General 30-Day Election Period

- Employees must have a period of at least **30 days** from the date of the event to enroll or change their election pursuant to a HIPAA special enrollment event
  - Longer periods would need to be approved by the insurance carrier or stop-loss provider

Medicaid/CHIP: Special 60-Day Election Period

- When employees lose Medicaid/CHIP eligibility, or where they gain eligibility for a state premium assistance subsidy under Medicaid/CHIP, they must have at least **60 days** from the date of the event to enroll or change their election
  - This is a good ERISA trivial pursuit question

HIPAA Special Enrollment Events

Effective Date: Generally First of the Month Following Election

- The general rule is that an election to enroll in coverage pursuant to a HIPAA special enrollment event must be effective no later than the first of the month following the date of the timely submitted election change request
  - **Example 1:** Jack marries Jill on April 19, and he submits the election change request to enroll Jill on April 22. Jill's coverage should be effective no later than May 1.
  - **Example 2:** Jack marries Jill on April 19, but does not submit the election change request to enroll Jill until May 14. Jill's coverage should be effective no later than June 1.

Birth/Adoption: Coverage Retroactive to the Date of the Event

- Where an employee has a new child through birth, adoption, or placement for adoption, coverage for the new child must be effective as of the date of the event
- In other words, coverage is effective the date of the birth, adoption, or placement for adoption
  - **Example:** Jack's spouse Jill gives birth to a child on July 19. Jack submits the election change to enroll the child on August 14. The child's coverage must be effective as of July 19 (the date of birth)

Existing Dependents: No Special Enrollment Rights

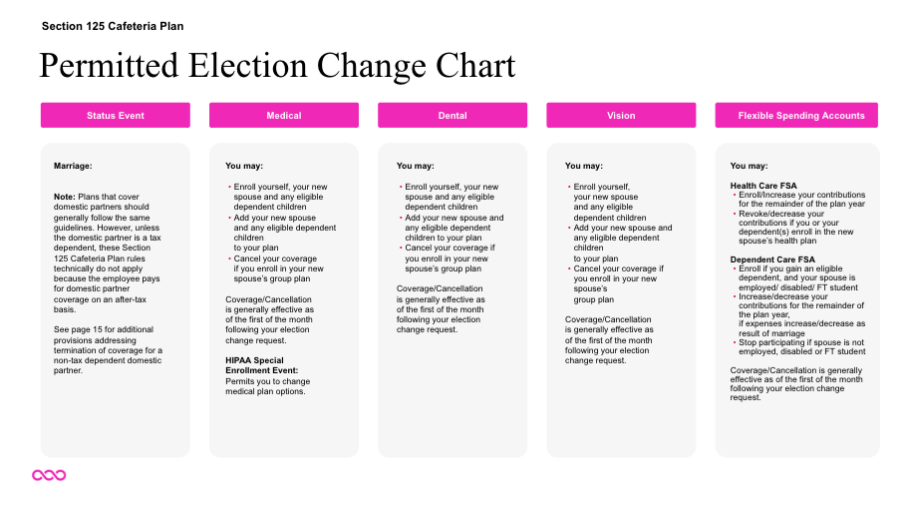
- Upon birth, the HIPAA rules limit the special enrollment rights to the employee, the spouse, and any newly acquired dependents (i.e., the newborn child)
- Any other dependents (e.g., siblings of the newborn child) are not entitled to special enrollment rights upon the employee's acquisition of the new dependent through birth
  - The exclusion of existing dependents from special enrollment rights prevents the employee from having the right to add an existing child to the plan upon the birth of the new child (optional cafeteria plan "tag-along" rule may permit enrollment)

HIPAA Special Enrollment Events

A Subset of Section 125 Events

Section 125 Cafeteria Plan Permitted Election Change Event Chart

Click here for a summary overview of the permitted election change events!



Section 125 Cafeteria Plan

Permitted Election Change Chart

Status Event	Medical	Dental	Vision	Flexible Spending Accounts
Marriage: **Note:** Plans that cover domestic partners should generally follow the same guidelines. However, unless the domestic partner is a tax dependent, these Section 125 Cafeteria Plan rules technically do not apply because the employee pays for domestic partner coverage on an after-tax basis. See page 15 for additional provisions addressing termination of coverage for a non-tax dependent domestic partner.	**You may:** • Enroll yourself, your new spouse and any eligible dependent children • Add your new spouse and any eligible dependent children to your plan • Cancel your coverage if you enroll in your new spouse's group plan Coverage/Cancellation is generally effective as of the first of the month following your election change request. **HIPAA Special Enrollment Event:** Permits you to change medical plan options.	**You may:** • Enroll yourself, your new spouse and any eligible dependent children • Add your new spouse and any eligible dependent children to your plan • Cancel your coverage if you enroll in your new spouse's group plan Coverage/Cancellation is generally effective as of the first of the month following your election change request.	**You may:** • Enroll yourself, your new spouse and any eligible dependent children • Add your new spouse and any eligible dependent children to your plan • Cancel your coverage if you enroll in your new spouse's group plan Coverage/Cancellation is generally effective as of the first of the month following your election change request.	**You may:** **Health Care FSA** • Enroll/Increase your contributions for the remainder of the plan year • Revoke/decrease your contributions if you or your dependent(s) enroll in the new spouse's health plan **Dependent Care FSA** • Enroll if you gain an eligible dependent, and your spouse is employed/ disabled/ FT student • Increase/decrease your contributions for the remainder of the plan year, if expenses increase/decrease as result of marriage • Stop participating if spouse is not employed, disabled or FT student Coverage/Cancellation is generally effective as of the first of the month following your election change request.

03

Health Status Nondiscrimination

Wellness Programs

Wellness Program HIPAA/ACA History

1996

HIPAA signed into law

2006

DOL/IRS/HHS regulations issued in 2006 applying HIPAA nondiscrimination rules to wellness programs

- HIPAA nondiscrimination rules generally prohibit group health plans from discriminating based on health-related factors with respect to premiums or cost-sharing
- Wellness program regulations designed as an exception to the HIPAA nondiscrimination rules for programs that meet the requirements in the regulations

2010

ACA codifies 2006 regulations into statute

- Generally without changes—except for increase to incentive limit from 20% to 30% (and 50% for tobacco cessation)
- Effective date: Plan years beginning on or after 1/1/14

2013

DOL/IRS/HHS issues new final regulations based on the ACA (which was primarily a codification of prior 2006 final regulations)

- Started with a statute (HIPAA), followed by regulations (2006), followed by codified regulations (ACA 2010), followed by regulations based on the codified regulations (2013)
- Plus, new 2013 final regulations claim application to grandfathered plans (even though the ACA specifically exempts) based on original HIPAA authority!

Federal Laws That May Apply to Wellness Programs

1. HIPAA Nondiscrimination (as modified by the ACA)
2. ADA
3. GINA
4. ACA Market Reforms
5. ERISA
6. COBRA
7. HIPAA Privacy/Security
8. More? (ADEA, FLSA, IRC)

Which Wellness Programs Must Comply?

The threshold issue for a wellness programs is to determine if it must comply with the HIPAA/ACA and the ADA requirements.

HIPAA/ACA Threshold Question

Is the wellness program a group health plan?

- An employee welfare benefit plan is a group health plan if it provides **"medical care"**
- "Medical care" generally refers to "the diagnosis, cure, mitigation, treatment, or prevention of disease, or amounts paid for the purpose of affecting any structure or function of the body"
- Most wellness programs will fall into this category of group health plan
- Any form of blood draws, screening, examinations, assessments, disease management, health incentives, or counseling by trained professionals likely triggers group health plan status
- Pure referral services, general information for mere promotion of good health, or basic educational sessions not customized to the employee likely are not a group health plan

ADA Threshold Question

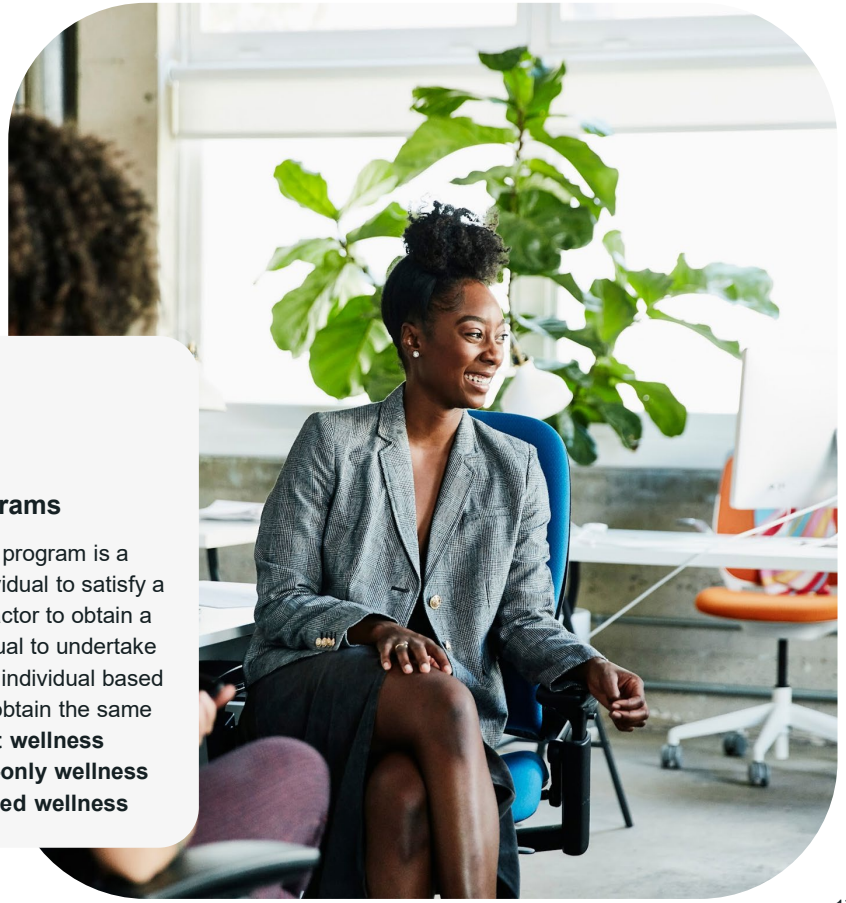
Does the wellness program include:

1. **Disability-related inquiries; and/or**
2. **Medical Examinations**

- The ADA rules apply to any wellness program that is an "**employee health program"** that asks employees to respond to disability-related inquiries and/or undergo medical examinations
- Includes wellness programs that are offered only to employees enrolled in the employer-sponsored group health plan, offered to all employees regardless of whether they enrolled in the employer's plan, or offered by employers that do not offer a group health plan
- Examples of "employee health programs" that may trigger the ADA regulations include health risk assessments (HRAs) to determine risk factors, medical screening for high blood pressure/cholesterol/glucose, classes to help employees stop smoking or lose weight, physical activities (e.g., walking or daily exercise), coaching to help employees meet health goals, and/or flu shots

Two Main Types of Wellness Programs

From the HIPAA Nondiscrimination Rules



Participatory Programs

"If **none of the conditions** for obtaining a reward under a wellness program is based on an individual **satisfying a standard that is related to a health factor** (or if a wellness program does not provide a reward), the wellness program is a participatory wellness program."

Health-Contingent Programs

"A health-contingent wellness program is a program that requires an individual to satisfy a standard related to a health factor to obtain a reward (or requires an individual to undertake more than a similarly situated individual based on a health factor in order to obtain the same reward). **A health-contingent wellness program may be an activity-only wellness program or an outcome-based wellness program."**

Two Main Types of Wellness Programs

Which Requirements Apply—HIPAA and ADA Overview

1. Participatory Programs

1. Program must be available to all similarly situated individuals
2. Program must be voluntary*
3. Program must provide reasonable accommodations*
4. Program must be reasonably designed to promote health or prevent disease*
5. Program reward/incentive is generally limited to 30% of the cost of coverage*
6. ADA wellness program notice provided to employees

2. Health-Contingent Programs

All six of the participatory program requirements, plus three more:

7. Program must offer individuals the opportunity to qualify for rewards at least once per year
8. Program must provide reasonable alternative standards (or waiver of standards) to obtain reward in certain situations
    - Significantly different rules apply for activity-only vs. outcome-based programs
9. HIPAA nondiscrimination wellness program notice describing reasonable alternative standards included in all plan materials describing the health-contingent wellness program

***Important note:** A federal court ruled in AARP v. EEOC that incentive components of the 2016 EEOC wellness program rules do not meet the requirements of the ADA, and that the EEOC must issue new regulations meeting certain standards. The EEOC accordingly formally removed those aspects of the regulations.

The EEOC issued new proposed regulations in January 2021 at the very end of the Trump administration that would have significantly changed the 2016 rules, however the Biden administration withdrew them shortly thereafter pursuant to a freeze on Trump regulations.

We feel that the best practice approach is to continue following the vacated 2016 EEOC regulations until we have new guidance specifying the ADA requirements moving forward. Regardless, the HIPAA nondiscrimination rules for wellness programs do remain in effect.

HIPAA Privacy/Security

01

Overview

Key Terms and Primary Responsibilities

HIPAA Privacy 101: Key Terms

Covered Entity 	• **Health Plan**
	  • Employer-sponsored group health plans
	  • Health insurance carriers (including HMOs)
	  • Medicare, Medicaid, VA, IHS, TRICARE, etc.
	• **Health Care Clearinghouse**
	• **Health Care Provider** (who transmits health information electronically)
	  • Doctors, nurses, hospitals, clinics, psychologists, dentists, chiropractors, nursing homes, pharmacies, etc.

Business Associate 	• An entity that performs a listed function or activity on behalf of a covered entity; and • Creates, receives, maintains, or transmits PHI on behalf of the covered entity • Examples: Claims processing, data analysis, utilization review, billing, legal, actuarial, accounting, consulting, data aggregation
Protected Health Information (PHI) 	• Individually identifiable health information maintained or transmitted by a Covered Entity or Business Associate • Excludes enrollment/disenrollment information used by the employer for employment purposes (that does not include any substantial clinical information)

HIPAA PHI

Individually identifiable health information maintained or transmitted by a Covered Entity or Business Associate

Common Examples of PHI	Common Examples of Items That Are Not PHI (And thus not subject to HIPAA privacy and security rules)

• Electronic claims information e-mailed to a group health plan by a Third-Party Administrator that contains identifiers
• An e-mail sent to an insurance carrier or Third-Party Administrator about an employee's claim that includes the health condition and an identifier
• A hard copy or electronic copy of an Explanation of Benefits
• A claims experience report kept in electronic format or hard copy that contains identifiers
• A transition of care form
• Health Risk Assessments
• Enrollment/disenrollment information maintained by a covered entity/business associate (i.e., not maintained by the employer as an employment record)
	• Employment/HR records with data not collected from a covered entity, including information to comply with other laws
	  • Such as information collected for FMLA, sick leave, or other similar leaves; alcohol and drug-free workplace law compliance; information required by Americans with Disabilities Act; fitness for duty reports
	• Health information from non-health care plans
	  • Such as STD/LTD; life insurance; AD&D; business travel accident; workers' compensation
	• General health care information
	  • Information that is not individually identifiable or did not come from a HIPAA covered entity/business associate

The BIG Exception– Enrollment/Disenrollment Information

The exclusion of enrollment/disenrollment information from the definition of PHI subject to all the HIPAA protection significantly limits the scenarios where HIPAA applies.

Enrollment Information: PHI?

- Employment records held by the covered entity **in its role as employer are <u>not</u>** PHI
  - This exclusion from PHI applies to enrollment and disenrollment information held by the employer
  - Such information cannot include any substantial clinical information to qualify for the PHI exemption
  - Significantly limits which and how often employers actually use or disclose PHI

- Enrollment and disenrollment information held by a covered entity (or business associate) **other than the employer <u>is</u>** PHI if created by or received from a covered entity (i.e., not from the employer in its role as employer)
  - Such entities are not the employer and therefore do not hold such information as employer records

The BIG Exception– Enrollment/Disenrollment Information

Relevant Cites

45 C.F.R. §160.103

(2) Protected health information excludes individually identifiable health information:

…

(iii) In employment records held by a covered entity in its role as employer

65 Fed. Reg. 82461, 82496

"Plan sponsors that perform enrollment functions are doing so on behalf of the participants and beneficiaries of the group health plan and not on behalf of the group health plan itself. For purposes of this rule, plan sponsors are not subject to the requirements of § 164.504 regarding group health plans when conducting enrollment activities."

67 Fed. Reg. 53181, 53208

"[T]he standard enrollment and disenrollment transaction does not include any substantial clinical information…However, the Department clarifies that, in disclosing or maintaining information about an individual's enrollment in, or disenrollment from, a health insurer or HMO offered by the group health plan, the group health plan may not include medical information about the individual above and beyond that which is required or situationally required by the standard transaction and still qualify for the exceptions for enrollment and disenrollment information allowed under the Rule."

Questions

What was the original purpose of the Health Insurance Portability and Accountability Act (HIPAA)?

Does HIPAA prohibit the use or disclosure of an individual's protected health information (PHI)?

Does HIPAA prohibit me from listening to someone tell me about their medical problem?

While doing my job, can I be held civilly and/or criminally responsible for a HIPAA violation?

HIPAA Privacy and Security

Why Should Plan Sponsors Care?

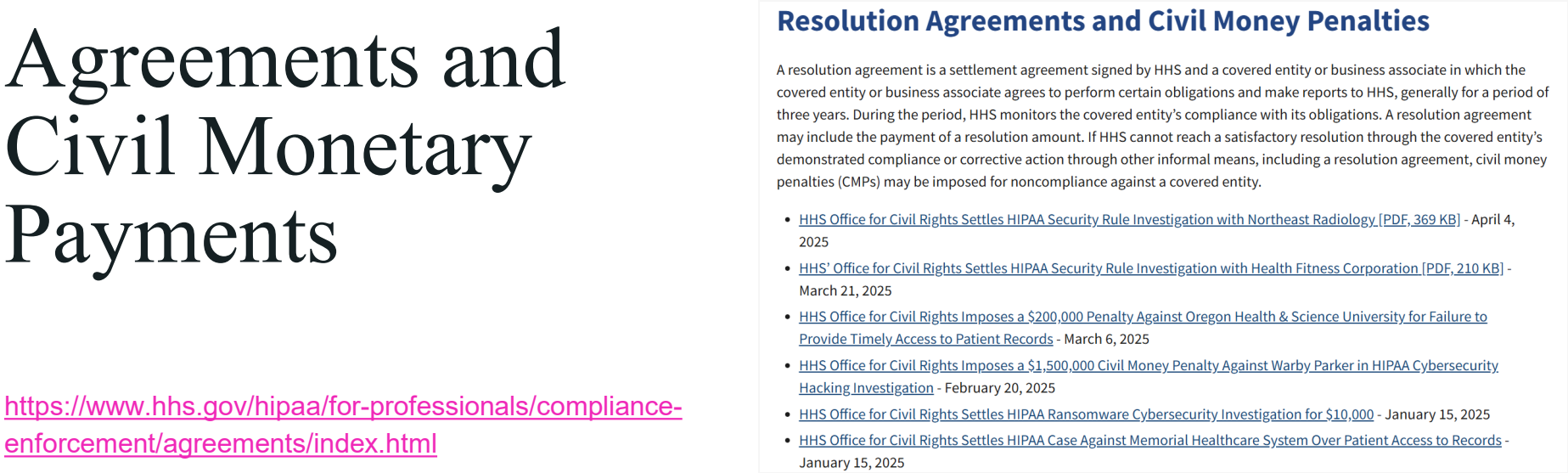
- Any employer that provides group health benefits is affected based on the level of exposure to PHI
  - Employers with self-insured plans effectively are directly subject to the rules
  - Even fully insured plans need to be sensitive to HIPAA
- Company access to employee health plan records for employment reasons (including administration of benefit plans) is severely limited
- Civil and criminal actions may be brought by HHS
  - If HHS fails to act, state attorney generals may bring civil suits
- Civil monetary penalties (indexed) can be assessed by HHS, and were significantly increased by HITECH

Culpability	Minimum Penalty per Violation	Maximum Penalty Per Violation	Annual Limit
No Knowledge	$141	$71,162	$25,000*
Reasonable Cause	$1,424	$71,162	$100,000*
Willful Neglect (Timely Corrected)	$14,232	$71,162	$250,000*
Willful Neglect (Not Corrected)	$71,162	$71,162	$1,500,000*

* Based on 2019 HHS enforcement policy that sets penalty caps below current indexed levels.

HHS Posts Resolution Agreements and Civil Monetary Payments

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html



Resolution Agreements and Civil Money Penalties

A resolution agreement is a settlement agreement signed by HHS and a covered entity or business associate in which the covered entity or business associate agrees to perform certain obligations and make reports to HHS, generally for a period of three years. During the period, HHS monitors the covered entity's compliance with its obligations. A resolution agreement may include the payment of a resolution amount. If HHS cannot reach a satisfactory resolution through the covered entity's demonstrated compliance or corrective action through other informal means, including a resolution agreement, civil money penalties (CMPs) may be imposed for noncompliance against a covered entity.

- HHS Office for Civil Rights Settles HIPAA Security Rule Investigation with Northeast Radiology [PDF, 369 KB] - April 4, 2025
- HHS' Office for Civil Rights Settles HIPAA Security Rule Investigation with Health Fitness Corporation [PDF, 210 KB] - March 21, 2025
- HHS Office for Civil Rights Imposes a $200,000 Penalty Against Oregon Health & Science University for Failure to Provide Timely Access to Patient Records - March 6, 2025
- HHS Office for Civil Rights Imposes a $1,500,000 Civil Money Penalty Against Warby Parker in HIPAA Cybersecurity Hacking Investigation - February 20, 2025
- HHS Office for Civil Rights Settles HIPAA Ransomware Cybersecurity Investigation for $10,000 - January 15, 2025
- HHS Office for Civil Rights Settles HIPAA Case Against Memorial Healthcare System Over Patient Access to Records - January 15, 2025

HIPAA Civil Liability Case Study #1

Medical Center's Unencrypted Laptop and Flash Drive

$3 Million HIPAA Settlement Agreement

- University Medical Center paid $3 million in November 2019 to the HHS OCR for two major breaches (2013 and 2017)
  - Unencrypted flash drive containing unsecured PHI lost in 2013
  - Unencrypted laptop of surgeon containing unsecured PHI stolen in 2017
- Severity in part because the Medical Center "failed to implement sufficient mechanisms to encrypt and decrypt ePHI"
- Also failed to implement security measures sufficient to reduce risks and vulnerabilities despite similar 2010 breach also involving a lost unencrypted flash drive and assistance from HHS OCR to improve policies

Bottom Line: Don't store unencrypted PHI on portable devices!

- HHS OCR: "Because theft and loss are constant threats, failing to encrypt mobile devices needlessly puts patient health information at risk…When covered entities are warned of their deficiencies, but fail to fix the problem, they will be held fully responsible for their neglect."
  - Full details: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/urmc/index.html

HIPAA Civil Liability Case Study #2

Dentist Discloses PHI of Patient on Social Media

$50,000 Civil Monetary Penalty

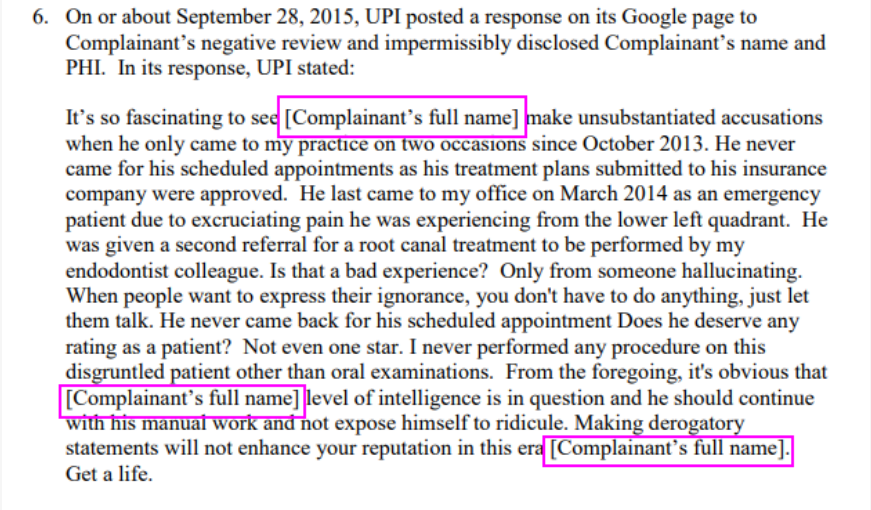
- Dental patient posted a negative review (using a pseudonym) of a North Carolina dentist in 2015 on the dentist's Google page
  - The dentist responded on the public google review site
  - Dentist's response impermissibly disclosed the patient's name and PHI
- Dentist did not respond to OCR's data request or subpoena, then waived rights to a heaving by not contesting the OCR findings

Bottom Line: Don't disclose PHI on public websites or social media!

- HHS OCR: "Here, UPI impermissibly disclosed the PHI of one individual, revealing his name, medical history, and the nature of his medical treatment. Despite repeated notice of this impermissible disclosure, UPI has not demonstrated any effort to mitigate any potential harmful effects of the impermissible disclosure or to come into compliance with the applicable provisions of the Privacy Rule by removing the PHI from its Google page."
  - Full details: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/upi/index.html

HIPAA Civil Liability Case Study

Dentist Discloses PHI on of Patient on Social Media



6. On or about September 28, 2015, UPI posted a response on its Google page to Complainant's negative review and impermissibly disclosed Complainant's name and PHI. In its response, UPI stated:

It's so fascinating to see [Complainant's full name] make unsubstantiated accusations when he only came to my practice on two occasions since October 2013. He never came for his scheduled appointments as his treatment plans submitted to his insurance company were approved. He last came to my office on March 2014 as an emergency patient due to excruciating pain he was experiencing from the lower left quadrant. He was given a second referral for a root canal treatment to be performed by my endodontist colleague. Is that a bad experience? Only from someone hallucinating. When people want to express their ignorance, you don't have to do anything, just let them talk. He never came back for his scheduled appointment Does he deserve any rating as a patient? Not even one star. I never performed any procedure on this disgruntled patient other than oral examinations. From the foregoing, it's obvious that [Complainant's full name] level of intelligence is in question and he should continue with his manual work and not expose himself to ridicule. Making derogatory statements will not enhance your reputation in this era [Complainant's full name]. Get a life.

HIPAA Civil Liability Case Study #3

Unauthorized Disclosure to Media of Photography of Patients Suffering from Covid

$80,000 HIPAA Settlement Agreement

- Saint Joseph's Medical Center shared photographs and other information to the Associated Press related to Covid
  - AP Exclusive: 'It's been a nightmare' for Yonkers ER doc
  - 'I needed to Tell Their Story' AP Staffer Captures ER Save
- Disclosure of three patients photographed was without their authorization
- HIPAA covered entities cannot disclose PHI to the media without first obtaining written authorization, even when reporters on site
- Medical Center paid $80,000 to OCR and agreed to implement a corrective action plan to comply with HIPAA going forward

Why Are the AP Materials Still Publicly Available?

- The media is not a HIPAA covered entity—it's the responsibility of covered entities (and their business associates) to use or disclose PHI only as permitted or required by HIPAA
- AP takes the position that the photos are important to tell frontline pandemic story to public—difficult moral questions here
  - Full details: https://www.hhs.gov/about/news/2023/11/20/hhs-office-civil-rights-settles-hipaa-investigation-st-josephs-medical-center-disclosure-patients-protected-health-information-news-reporter.html

HIPAA Civil Liability Case Study #4

Ransomware Attack at Business Associate from Phishing Email

$240,000 Civil Monetary Penalty

- Physician group (covered entity) with 35 medical offices engaged with IT vendor for data management services (business associate)
  - The physician group failed to enter into a business associate agreement (BAA) with the IT vendor
  - Employee at one of the physician group divisions clicked on a phishing email, allowing hackers to gain remote access to PHI
- Resulted in three waves of ransomware attacks that compromised the PHI of 85,000 individuals
- The compromised PHI included names, addresses, dates of birth, driver's license numbers, Social Security numbers, lab results, medications, treatment information, credit card information, bank account numbers, and other financial information.

Bottom Line: Ensure BAAs are in place with business associates (outside vendors that have access to PHI)

- HHS OCR: "While OCR acknowledges that PMI took some corrective actions to resolve the potential noncompliance during OCR's investigation, PMI/COS failed to have a Business Associate Agreement in place with its IT vendor for many years and its access control deficiencies contributed to the ransomware attacks."
  - Full details: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/pmi-nfd/index.html

HIPAA Civil Liability Case Study #5

Reproductive Health Disclosure Without Authorization

$35,581 HIPAA Settlement Agreement

- Medical practice in Pennsylvania received an authorization from a patient to release one specific test result to prospective employer
  - The medical practice erroneously provided the prospective employer with the patient's entire medical record
  - Included surgical history, genealogical history, obstetric history, and other sensitive PHI concerning reproductive health care
- The medical practice did not have the patient's authorization for the broad disclosure of her PHI, and there otherwise was no applicable permission under HIPAA for such a broad release of her medical records
- On top of the settlement payment, the group agreed to a multi-step Corrective Action Plan to be monitored by HHS OCR for the next two years to ensure this type of breach never occurs again

Bottom Line: Do not disclose PHI beyond the specific information set forth in an authorization—especially sensitive PHI

- HHS OCR: "Patients must be able to trust that sensitive, health information in their files is protected to preserve their trust in the patient-doctor relationship and ensure they get the care they need. This is particularly true for reproductive health privacy."
  - Full details: https://www.hhs.gov/about/news/2024/11/26/hhs-office-civil-rights-settles-holy-redeemer-hospital-disclosure-patients-protected-health-information-including-reproductive-health-information.html

HIPAA Privacy and Security

Why Should Plan Sponsors Care?

Potential Criminal Penalties

- Covered entities, business associates, and their employees can be held criminally liable for **knowingly violating HIPAA**

These criminal penalties apply only where there is criminal intent

- Inadvertent mistakes with respect to HIPAA are not the concern here
- HIPAA prosecutions occur for situations like identity theft, selling celebrity medical information to the media, Medicare fraud, accessing PHI of individuals the medical practitioner is not treating, etc.

Aggravating Circumstances	Maximum Fine	Maximum Imprisonment
General “Knowingly” Standard	$50,000	One Year
False Pretenses	$100,000	Five Years
Intent to Sell, Transfer, or Use PHI for Commercial Advantage, Personal Gain, or Malicious Harm	$250,000	Ten Years

02

HIPAA Privacy

HIPAA Privacy Overview

Patients Have the Right to Understand and Control How Their Health Information Is Being Used

- **Notice of Privacy Practices:** Providers and health plans to give individuals clear, written notice of how they use, keep, and disclose their health information
- Individuals have right to access their medical records (to view, make copies, request amendments, and obtain accounting for non-routine disclosures)
- Individual authorizations required before information is released in most non-routine situations
- Covered entities accountable for use and release of information, with recourse available if privacy is violated

Use of Individual Health Information Generally Limited to Health Purposes

- PHI generally cannot be used for purposes other than **"treatment," "payment," or "health care operations"** without individual authorization
- Individual authorizations must be informed and voluntary
  - Most insurance carriers require use of HIPAA authorizations prior to disclosing PHI with respect to a participant enrolled in an insured group health plan
- **Minimum Necessary Rule:** Reasonable efforts must be undertaken to limit release of information to "minimum necessary amount"
  - Minimum necessary amount requirement applies to use of protected health information for payment or health plan operations, but not for treatment purposes

The Big Three Permitted Uses of PHI

HIPAA permits covered entities to use or disclose PHI for three different reasons without requiring the individual's authorization. These three items are disclosed in the covered entity's notice of privacy practices and permit the health care industry to function smoothly.

1

Treatment

- Providing of care by health care providers
- Does not apply to health plan covered entities (including employers)
- Remember that the minimum necessary rule does not apply to treatment

2

Payment

- To obtain premiums, determine or fulfill responsibility for coverage and provision for benefits under the health plan, to provide reimbursement
- Includes eligibility determinations, subrogation, risk adjusting, billing, claims management, collection, stop-loss, medical necessity and utilization review

3

Health Care Operations

- Quality assessment and improvement, patient safety activities, case management, care coordination, information about treatment alternatives
- Underwriting, enrollment, premium rating, and other contractual processes, customer service, plan sponsor data analysis, wellness program operations

HIPAA Privacy Overview

Key Points to Remember

Minimum privacy safeguard standards established for covered entities (with similar requirements applicable to business associates and, in some situations, even plan sponsors).

Adoption of privacy procedures, with safeguards and sanctions specified

Periodic distribution of privacy notice

Training of employees on handling PHI

Designation of a privacy officer

Establishment of a grievance / complaint procedure

Recordkeeping with respect to PHI disclosures

HIPAA Privacy Overview

Fully Insured Plans: Reduced Compliance Burden

- With fully insured plans, both the group health plan and the insurance carrier are HIPAA covered entities
- **Generally, employers sponsoring a fully insured plan do not need HIPAA policies and procedures documents, to provide employees with a notice of privacy practices, to engage in business associate agreements, or undergo HIPAA training**
  - The insurance carrier is directly responsible for those requirements
- Applies where employers receive only summary health information for limited purposes and enrollment/disenrollment information
- Most employers offer a health FSA, which is a self-insured group health plan that technically is directly subject to these HIPAA requirements
  - From a practical perspective, it is common for employers not to take all of the HIPAA steps described above (other than entering into a BAA with the TPA for the health FSA) where the only self-insured group health plan is the health FSA—although no technical exemption exists
- **Employers with a self-insured medical plan clearly do not enjoy this exemption from documentation, disclosure, and training requirements**

When is Training Required?

HIPAA is the only required employee benefits training! But there are a number of restrictive qualifications that significantly limit which employees actually need the training.

Only Employers

With Self-Insured Health Plan

- Employers with fully insured plans are not required to train employees
- Training not required because such employers receive only summary health information for limited purposes and enrollment/disenrollment information

Only Employees

Within the HIPAA Firewall

- Only those employees with a plan-related need to access PHI for plan administrative functions are within the HIPAA firewall
- These are the only employees who have access to PHI—and therefore the only employees who need training in how to handle PHI
- Generally required only for benefits and HR professionals
- Finance, accounting, payroll, C-suite, etc. generally do not need training (because they access only enrollment/disenrollment information that is not PHI as employment records)

Only New Hires

& Upon a Material Change in Policies and Procedures

- Training required within a “reasonable period of time” after hire
- After the initial training, re-training required only upon a material change in the plan’s HIPAA privacy policies and procedures
- Best practice: Retrain once every two years regardless of changes

Working with Vendors (Business Associates)

When is a BAA Required for Self-Insured Plans?

- HIPAA business associates can include third-parties in many different areas that create, receive, maintain, or transmit Personal Health Information
- **Examples include (but are not limited to):**
  - Claims processing or administration, data analysis, legal, actuarial, accounting, consulting, data aggregation, administrative, financial services
- Employers cannot permit such third-party vendors (business associates) to access PHI under their self-insured plan without entering into a business associate agreement (BAA) on behalf of the health plan (the HIPAA covered entity)
  - Fully insured plans generally do not need HIPAA BAAs
  - Note that enrollment/disenrollment information maintained by the employer (that does not include any substantive clinical information) is not PHI
- BAA will impose certain required safeguards on the business associates related to HIPAA privacy and security compliance
  - Note that the HITECH Act also imposes direct HHS liability on business associates—regardless of the terms of the BAA

Disclosing PHI to Family Members

General rule is that the individual must authorize disclosure of PHI that is not to a covered entity or business associate for treatment, payment, or health care operations.

In some limited situations, the covered entity (e.g., the health plan) may disclose PHI to a family member or close personal friend **if the PHI is directly relevant** to their involvement to assist in the individual's care or payment.

This issue often arises with parents assisting a pre-26 adult child with treatment/payment.

Individual Has Capacity to Make Health Care Decision

Covered entity may disclose if:

- Obtains agreement (written or oral) from the individual;
- Provides the individual with the opportunity to object to the disclosure (and the individual does not object); OR
- Reasonably infers from the circumstances, based on exercise of professional judgment, that the individual does not object to the disclosure

Individual Not Present, Incapacitated, or Emergency

Covered entity may disclose if:

- In the exercise of professional judgment determines that the disclosure **is in the best interests** of the individual; **AND**
- Limits disclosure to only the PHI that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes

Disclosing PHI to Family Members

May a health plan disclose protected health information to a person who calls the plan on the beneficiary's behalf?

Answer:

Yes, subject to the conditions set forth in 45 CFR 164.510(b) of the HIPAA Privacy Rule. The Privacy Rule at 45 CFR 164.510(b) permits a health plan (or other covered entity) to disclose to a family member, relative, or close personal friend of the individual, the protected health information (PHI) directly relevant to that person's involvement with the individual's care or payment for care. A covered entity also may make these disclosures to persons who are not family members, relatives, or close personal friends of the individual, provided the covered entity has reasonable assurance that the person has been identified by the individual as being involved in his or her care or payment.

A covered entity only may disclose the relevant PHI to these persons if the individual does not object or the covered entity can reasonably infer from the circumstances that the individual does not object to the disclosure; however, when the individual is not present or is incapacitated, the covered entity can make the disclosure if, in the exercise of professional judgment, it believes the disclosure is in the best interests of the individual.

For example:

- A health plan may disclose relevant PHI to a beneficiary's daughter who has called to assist her hospitalized, elderly mother in resolving a claims or other payment issue.
- A health plan may disclose relevant PHI to a human resources representative who has called the plan with the beneficiary also on the line, or who could turn the phone over to the beneficiary, who could then confirm for the plan that the representative calling is assisting the beneficiary.
- A health plan may disclose relevant PHI to a Congressional office or staffer that has faxed to the plan a letter or e-mail it received from the beneficiary requesting intervention with respect to a health care claim, which assures the plan that the beneficiary has requested the Congressional office's assistance.
- A Medicare Part D plan may disclose relevant PHI to a staff person with the Centers for Medicare and Medicaid Services (CMS) who contacts the plan to assist an individual regarding the Part D benefit, if the information offered by the CMS staff person about the individual and the individual's concerns is sufficient to reasonably satisfy the plan that the individual has requested the CMS staff person's assistance.

https://www.hhs.gov/hipaa/for-professionals/faq/1067/may-a-health-plan-disclose-information-to-a-person-who-calls/index.html

03

HIPAA Security

HIPAA Security Overview

Key points to remember

Establishes three primary standards (**administrative safeguards, physical safeguards, and technical safeguards**) with various required or addressable implementation specifications

- Reflects commonly accepted IT security safeguards widely used across many industries

Security measures to be tailored to organization's risk analyses, technical environment, and business needs

- Must be flexible and dynamic, while being reasonable and scalable
- High premium on documentation of decision process and implementation of risk assessment and appropriate countermeasures

HIPAA Workforce Members

The HIPAA Firewall

- HIPAA firewall should ensure that only those employees with a plan-related need to access PHI for plan administrative functions are permitted access to the plan's PHI
  - Plan administration functions include payment and health care operations activities performed by employees of the employer
  - Does not include employee enrollment and disenrollment information maintained by the employer (that does not include substantial clinical information) because such information is not PHI protected by HIPAA
- **Among other concerns, this ensures no PHI is used for employment-related purposes—which is strictly prohibited by HIPAA**
- Employers need to keep access to electronic information, paperwork, and conversations that include PHI restricted to only those workforce members with a plan-related need to know the information (the HIPAA firewall)
  - The wrap plan document should include standard HIPAA provisions certifying that the employer will follow these HIPAA firewall restrictions in its use and disclosure of PHI

HIPAA Workforce Members

The HIPAA Firewall

Open Workspaces & Hotel Seating vs. The HIPAA Firewall

Benefits professionals should be careful to limit their conversations and documents that include PHI to private offices, conference rooms, call rooms, or other private areas that are available on-demand

- Keep in mind that employee enrollment and disenrollment information maintained by the employer (that does not include substantial clinical information) is not PHI protected by HIPAA
- This should limit the frequency in which PHI will be viewed or discussed by employees within the firewall whose job duties are related to the plan

Avoiding PHI Issues: De-Identification

De-identified information is not PHI

- De-identified health information cannot be used to identify an individual
- Can be no reasonable basis to believe that the information can be used to identify the individual
- Must remove 18 specific identifiers for the information to be “de-identified” and non-PHI that is not subject to these HIPAA restrictions

De-Identified HIPAA PHI

De-Identified Information Must Remove 18 Identifiers from PHI

1. Names
2. Geographic divisions smaller than a State:
   - Address, city, county, precinct, zip code, geocode
   - Initial three digits of zip code may be included with restrictions
3. All dates more precise than the year:
   - Date of birth/death, admission/ discharge date, all ages over 89
4. Phone numbers
5. Fax numbers
6. Email addresses
7. SSNs
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers:
    - Serial/license plate numbers
13. Device identifiers and serial numbers
14. URLs
15. IP address numbers
16. Biometric identifiers:
    - Fingerprints, voice prints
17. Full face pictures and anything comparable
18. Any other unique identifying number, characteristic, or code

New DOL Guidance on Cybersecurity

Full Details: Compliance Assistance Release No. 2024-01

The DOL put out cybersecurity guidance in 2021 that was widely regarded as directed toward retirement plans. In 2024, the DOL clarified that employers have the same fiduciary responsibility to include cybersecurity matters as part of the process to prudently select and monitor vendors for non-retirement plan benefits.

- *The guidance provides a useful set of materials that employers can use to satisfy the fiduciary standards for cybersecurity.*

Tips for Hiring a Service Provider:

- A number of tips for employers of all sizes and for all types of ERISA plans for what to ask and evalutate with respect to any service provider's cybersecurity practices.

Also includes suggested contractual terms:

- Information Security Reporting
- Clear Provisions on the Use and Sharing of Information and Confidentiality
- Notification of Cybersecurity Breaches
- Compliance with Records Retention and Destruction, Privacy and Information Security Laws
- Insurance

Cybersecurity Best Practices:

- 12 best practice approaches for plan service providers to ensure proper mitigation of cybersecurity risks.

Includes the following key themes:

- Identify the risks to assets, information and systems
- Protect each of the necessary assets, data and systems
- Detect and respond to cybersecurity events
- Recover from the event
- Disclose the event as appropriate
- Restore normal operations and services

Online Security Tips:

Tips for employees to reduce the risk of fraud and loss online:

- Register, set up and routinely monitor your online account
- Use strong and unique passwords/passphrases
- Use Multi-Factor Authentication
- Keep personal contact information current
- Close or delete unused accounts
- Be wary of free wi-fi
- Beware of phishing attacks
- Use antivirus software and keep apps and software current

04

Compliance Strategies

Compliance Strategies

Review of Basic Standards to Follow in Day-to-Day Practice

- PHI and e-PHI must remain confidential and may only be used for the purpose it was made available to you
- Do not share PHI and e-PHI with unauthorized individuals (even including co-workers who have no plan-related need to know)
- Do not share or discuss PHI or e-PHI with a friend or spouse
- Use physical safeguards to protect PHI and e-PHI (e.g., locking all files that contain PHI; “clean desk” policies; using only assigned and secure fax machines; not taking PHI or e-PHI home in files or on flash drives or laptops)
- Use electronic safeguards to protect e-PHI (e.g., only store e-PHI on network drives that are frequently backed up and subject to electronic protection; encrypt non-network stored e-PHI)
- In transmitting e-PHI by e-mail, use encryption
- Identify and limit, to the extent possible, transmission of e-PHI through potentially unsecured medium (such as computers, PDAs, flash drives, servers, and other electronic devices)
- If you receive an e-mail containing PHI that is **not** adequately protected, then follow these steps:
  - Notify the person who sent the e-mail message that e-PHI was not adequately protected, that you will be deleting his/her e-mail message, and that e-PHI should be re-sent to you through a secure medium
  - If person sends e-PHI multiple times without adequate protection, then your HIPAA privacy policy will likely require filing a report with your Privacy Official

HIPAA and Part 2: Substance Use Disorder Protections

Court Case Removes Reproductive Health Rules

However, the Substance Use Disorder Provisions Remain in Effect

Purl v. United States HHS, No. 2:24-CV-228-Z, 2025 U.S. Dist. (N.D. Tex. June 18, 2025)

In sum, HIPAA confers authority to promulgate regulations protecting "individually identifiable health information." 42 U.S.C. § 1320d-2 note. But it confers no authority to distinguish between types of health information to accomplish *political* ends like protecting access to abortion and gender-transition procedures. Thus, HHS lacks the authority to issue regulations that enact heightened protections for information about politically favored procedures. "[T]he people and their elected representatives" remain free to enact their preferred protections for such procedures. *Dobbs*, 597 U.S. at 292. And HIPAA and its regulations cannot preempt any state laws that enact "more stringent" protections. *See* Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033–34 (1996).

But until the people speak through their representatives, agencies must fall silent on issues of abortion or other matters of great political significance. Thus, HHS lacked the authority to promulgate the 2024 Rule.

The court decision vacated the portion of the rules related to reproductive health, but severed that portion and preserved the other piece related to the Part 2 Rule for substance use disorder protections:

Fed. Reg. at 33048. The remainder of the changes to Section 164.520 in 89 Fed. Reg. 32976 are not "directly related" to the 2024 Rule's unlawful provisions. 89 Fed. Reg. at 33048. Thus, HHS intended them to sever.

Accordingly, 45 C.F.R. Section 164.520 is severed and not vacated *except* 45 C.F.R. Section 164.520(b)(1)(ii)(F), (G), and (H), which are vacated because HHS did not intend they remain.

The Part 2 Rule: Substance Use Disorder Protections Notice of Privacy Practices Update Required

What is the Part 2 Rule?

- Protects the records of the identity, diagnosis, prognosis, or treatment of any patient in connection with any federal program or activity relating to substance use disorder (SUD)
- Includes education, prevention, training, treatment, rehabilitation, or research
- Designed to address concerns that discrimination and fear of prosecution might deter treatment for SUD

What's New With Part 2?

- The CARES Act required the Part 2 rules to be more aligned with the HIPAA rules
- Final Part 2 rules issued February 8, 2024 completed that alignment
- Authority to enforce Part 2 rules was formally delegated to HHS OCR as of August 27, 2025
- Was initially in combination with reproductive health rules, *but a court vacated the reproductive health components*

The Action Item

Notice of Privacy Practices (NPP) Update by 2/16/26

- Originally the new Part 2 rules were largely addressed with the reproductive health rules that required a new attestation and NPP updates
- After the court decision, only the Part 2 SUD piece remains
- Requires NPP update by February 16, 2026 to reflect new SUD rights (but no longer includes reproductive health)

HIPAA HITECH Act

HIPAA – HITECH Act

Enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act has generated renewed interest in HIPAA privacy and security compliance.

Expanded various HIPAA privacy and security provisions (e.g., extended certain HIPAA obligations directly to business associates, implemented certain breach notification rules, increased penalties)

Staggered effective dates for various aspects of HITECH, but most become effective as of 2/17/10

Was incorporated into the American Recovery and Reinvestment Act (ARRA or “the stimulus bill”), which was enacted within the first month of President Obama taking office (2/17/09)

What is a Breach?

“Breach” Means

- Acquisition, access, or use, or disclosure of unsecured PHI in a manner not permitted, which compromises the security or privacy of the protected health information
- An impermissible use or disclosure is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the protected health information has been compromised
- Based on a risk assessment of the following factors:
  - The nature and extent of the PHI involved
  - The unauthorized person who used or had access to the PHI
  - Whether the PHI was actually acquired or viewed
  - The extent to which the risk to the PHI has been mitigated

“Breach” Excludes

- Unintentional acquisition, access, or use of PHI by person acting under authority of group health plan or business associate
- Inadvertent disclosure by a person authorized to access PHI to another person authorized to access PHI
- Disclosure of PHI where a group health plan or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the PHI

Breach Notification

Whenever a health plan discovers a breach of unsecured PHI, HITECH now requires notification to certain persons **without unreasonable delay** (and in no event later than 60 calendar days after discovery of breach).

Notice to Affected Individuals

- In writing by first-class mail (or by email, if individual has agreed)
- By conspicuous posting on website (called “substitute notice”), if contact information is insufficient or out-of-date
- In urgent situations (i.e., possible imminent misuse of unsecured PHI), by telephone or other appropriate means

Content of Notice to Affected Individuals

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
2. A description of the types of unsecured PHI that were involved in the breach (such as whether full name, SSN, DOB, home address, account number, diagnosis, disability code, or other types of information were involved);
3. Any steps the individuals should take to protect themselves from potential harm resulting from the breach;
4. A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and
5. Contact procedures for individuals to ask questions or learn additional information, including toll-free phone number, email address, website, or postal address

Breach Notification

Whenever a health plan discovers a breach of unsecured PHI, HITECH now requires notification to certain persons **without unreasonable delay** (and in no event later than 60 calendar days after discovery of breach).

Notice to Media

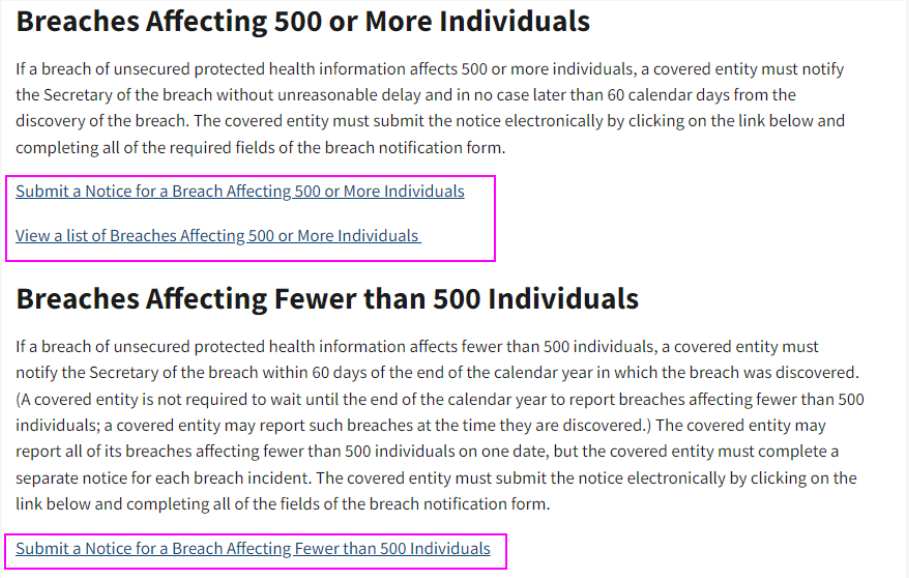
- For breach involving 500 or more individuals, notify “prominent media outlets” serving the state or jurisdiction
  - Without unreasonable delay (and in no event later than 60 calendar days after discovery of the breach)

Notice to U.S. Department of Health and Human Services (HHS)

- For breach involving 500 or more individuals, notify HHS as specified on HHS website
  - Without unreasonable delay (and in no event later than 60 calendar days after discovery of the breach)
- For breach involving less than 500 individuals, maintain a log and provide notice to HHS within 60 days after each calendar year

Breach Notification

https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html



Breaches Affecting 500 or More Individuals

If a breach of unsecured protected health information affects 500 or more individuals, a covered entity must notify the Secretary of the breach without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach. The covered entity must submit the notice electronically by clicking on the link below and completing all of the required fields of the breach notification form.

Submit a Notice for a Breach Affecting 500 or More Individuals

View a list of Breaches Affecting 500 or More Individuals

Breaches Affecting Fewer than 500 Individuals

If a breach of unsecured protected health information affects fewer than 500 individuals, a covered entity must notify the Secretary of the breach within 60 days of the end of the calendar year in which the breach was discovered. (A covered entity is not required to wait until the end of the calendar year to report breaches affecting fewer than 500 individuals; a covered entity may report such breaches at the time they are discovered.) The covered entity may report all of its breaches affecting fewer than 500 individuals on one date, but the covered entity must complete a separate notice for each breach incident. The covered entity must submit the notice electronically by clicking on the link below and completing all of the fields of the breach notification form.

Submit a Notice for a Breach Affecting Fewer than 500 Individuals

Annual Report to Congress on HIPAA Breaches (Most Recent: 2022 Calendar Year)

HHS Office for Civil Rights
Breach Reports of Unsecured PHI Affecting 500 or more Individuals in 2022 by Percentage of Reports Received by Entity Type

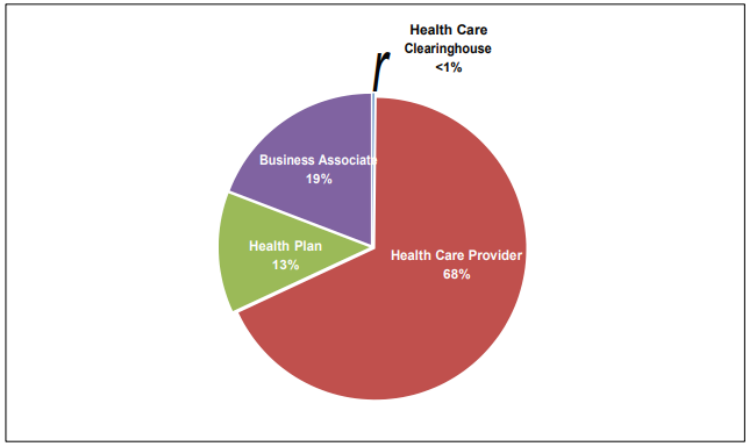


Figure 1

HHS Office for Civil Rights
Breach Reports of Unsecured PHI Affecting 500 or more Individuals in 2022 by Percentage of Reports Received by Type of Breach

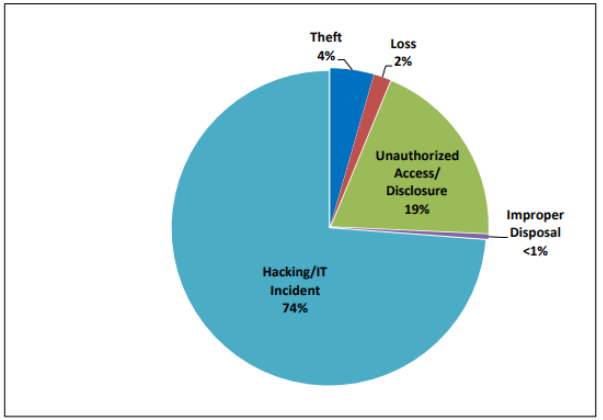


Figure 3

https://www.hhs.gov/hipaa/for-professionals/breach-notification/reports-congress/index.html

HIPAA

Quick Employer Checklist for Self-Insured Plans

HIPAA Self-Insured Checklist

Administrative	
Appoint a HIPAA Privacy Official	• Typically listed by title (rather than name) in HIPAA materials
Determine Which Employees Will Have Access to PHI	• This defines the HIPAA firewall • Should be limited to employees with a plan administrative functions • Remember this generally does not include enrollment/disenrollment information • Key point: Employees who wear HR and HIPAA hats must be careful never to permit PHI to be used or disclosed for employment-related purposes
Implement Routine Training Schedule	• Rule of thumb for employees within the HIPAA firewall at an employer: • Train within a reasonable period after hire and refresh training every two years • Only those within the HIPAA firewall need HIPAA training
Clean Desks, Locked Files, Secure Fax	• Don't leave PHI visible, lock hard copies of PHI, don't use main fax line for PHI
Documentation	
Establish HIPAA Policies and Procedures	• Internal document governing use and disclosure of PHI
Distribute Notice of Privacy Practices (NPP)	• Employee-facing document summarizing policies and procedures • Re-distribute within 60 days of a material change *(new changes needed by February 2026)* • Provide notice of availability of the NPP at least once every three years
Enter Into Business Associate Agreements (BAAs)	• Required for most third-party plan service providers with access to PHI • Newfront generally needs a BAA as consultant for a self-insured major medical
Plan Document and SPD HIPAA Provisions	• Ensure wrap plan document and wrap SPD in place with standard provisions governing employer responsibilities with respect to PHI

Don’t Forget: Document Training

Template Employee HIPAA Training Sign-in Sheet

Click here for a fillable pdf employee sign in sheet you can use!

NEWFRONT

Employee HIPAA Training Sign-In Sheet

Topic: HIPAA Privacy and Security Training

Presenter: Brian Gilmore, Newfront Lead Benefits Counsel

Date: **Time:**

	Employee Name	Employee Signature
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

WRAP-UP

Takeaways

HIPAA Training for Employers – From Portability to Privacy

THREE KEY POINTS TO REMEMBER

1

HIPAA includes two major branches: Portability and Privacy. Although some features are now obsolete, the HIPAA portability rules remain relevant and important today with respect to special enrollment events and nondiscrimination based on health status for wellness programs.

2

The HIPAA privacy and security rules are important for employers, especially employers with self-insured group health plans. These employers should designate a privacy official, create policies and procedures, distribute a notice of privacy practices (updated by Feb. 2026), and enter into BAAs with business associates. Employers should also be familiar with the HITECH Act breach rules.

3

Employees who are within the HIPAA firewall of a self-insured group health plans are required to undergo HIPAA training within a reasonable time after joining the workforce and within a reasonable time after any material change in policies and procedures. Don't forget to document that the training has been completed to comply with the HIPAA requirement to maintain documentation of training.

Content Disclaimer

HIPAA Training for Employers

The intent of this analysis is to provide the recipient with general information regarding the status of, and/or potential concerns related to, the recipient's current employee benefits issues. This analysis does not necessarily fully address the recipient's specific issue, and it should not be construed as, nor is it intended to provide, legal advice. Furthermore, this message does not establish an attorney-client relationship. Questions regarding specific issues should be addressed to the person(s) who provide legal advice to the recipient regarding employee benefits issues (e.g., the recipient's general counsel or an attorney hired by the recipient who specializes in employee benefits law).

Newfront makes no warranty, express or implied, that adherence to, or compliance with any recommendations, best practices, checklists, or guidelines will result in a particular outcome. The presenters do not warrant that the information in this document constitutes a complete list of each and every item or procedure related to the topics or issues referenced herein. Federal, state or local laws, regulations, standards or codes may change from time to time and the reader should always refer to the most current requirements and consult with their legal and HR advisors for review of any proposed policies or programs.

Thank you

Brian Gilmore

Lead Benefits Counsel, VP

brian.gilmore@newfront.com