HIPAA PRIVACY AND SECURITY

The New Final Regulations
Overview

- Background
- Recent Changes to HIPAA
- Identifying Business Associates
- Enforcement
- How to Report a Breach
- Frequently Asked Questions
HIPAA

♦ Health Insurance Portability and Accountability Act of 1996

♦ The Privacy Rule requires Covered Entities and their Business Associates to protect the privacy of protected health information (PHI) in any form

♦ The Security Rule requires Covered Entities and their Business Associates to protect the confidentiality, integrity and availability of electronic protected health information (ePHI)
HIPAA Applies To Covered Entities

- Health Care Providers (who conduct certain types of electronic transactions)
- Health Care Clearing Houses (who convert another entity’s health care transactions into standard format)
- Medicare Prescription Drug Card Sponsors
- Health Insurance Issuers, Medicare and Medicaid
- Group Health Plans
- Some provisions also apply to Business Associates
Group Health Plan

♦ All group health plans are Covered Entities (regulations use COBRA definition)

■ Exception for plans with fewer than 50 participants and self-administered
**Group Health Plan**

<table>
<thead>
<tr>
<th>Health Benefits Offered under a Typical Health and Welfare Benefits Plan Covered by HIPAA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical</td>
</tr>
<tr>
<td>Prescription Drugs</td>
</tr>
<tr>
<td>Dental</td>
</tr>
<tr>
<td>Behavioral Health</td>
</tr>
<tr>
<td>Health Care FSA</td>
</tr>
<tr>
<td>Vision</td>
</tr>
<tr>
<td>Long-Term Care</td>
</tr>
<tr>
<td>Employee Assistance Program</td>
</tr>
<tr>
<td>Wellness</td>
</tr>
<tr>
<td>Health Reimbursement Account</td>
</tr>
</tbody>
</table>
## Not Group Health Plan Benefits

<table>
<thead>
<tr>
<th>Benefits Offered under a Typical Health and Welfare Benefits Plan Not Covered by HIPAA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Life and Accidental Death and Dismemberment Insurance</td>
</tr>
<tr>
<td>Voluntary Permanent Life Insurance</td>
</tr>
<tr>
<td>Dependent Care FSA</td>
</tr>
<tr>
<td>Prepaid Legal</td>
</tr>
<tr>
<td>Pension Plans including disability determinations</td>
</tr>
<tr>
<td>Short-Term Disability</td>
</tr>
<tr>
<td>Long-Term Disability</td>
</tr>
<tr>
<td>Workers’ Compensation</td>
</tr>
<tr>
<td>Cash-Out Dollars for Waiving Benefits</td>
</tr>
<tr>
<td>Automotive and Homeowners Insurance</td>
</tr>
</tbody>
</table>
Protected Health Information

- **Protected Health Information (PHI)**
  - Health-related information about a person
  - Created or received by a Covered Entity such as a health plan
  - Could be used to identify the person
  - Includes demographic information (such as address and birth date)

- **Electronic Protected Health Information (ePHI)**
  - PHI that is stored, maintained or transmitted electronically

- **Examples of PHI**
  - Enrollment data, employee contribution information
  - Claims information and history
Not PHI

PHI does not Include Individually Identifiable Health Information in “Employment Records” or Benefits that are not Health Benefits

- Fitness for Duty Information
- Drug Screening
- FMLA
- OSHA
- Workers’ Compensation
- Life and Accidental Death and Dismemberment
- Long-Term Disability
- Long-Term Disability
- Short-Term Disability
- Dependent Care FSA
- Business Travel Assistance
- 401(k) Plan
- Pension Plan

STILL KEEP THIS INFORMATION CONFIDENTIAL!
Role of Employer

- Employer not a Covered Entity but may be subject to privacy requirements as health plan administrator through plan amendment

- Obligation to comply with HIPAA for employer depends on whether health plan is insured and if employer has access to PHI
Employer Obligations

- If plan is self-funded or employer has access to PHI:
  - HIPAA Privacy Notice Distribution
  - Plan Amendment
  - Erect “firewalls” between “plan” and “employer” functions
  - Administrative requirements for plan functions performed plan workforce
    - Written Policies and Procedures
    - Security Risk Assessment
    - Business Associate Agreements
    - Access, Amendment and Accounting Rights
    - Train Workforce Members
    - Recordkeeping
    - Appoint Privacy and Security Officials
Separation of Information

- Plan cannot share PHI with Employer in its role as Plan Administrator unless:
  - Plan Sponsor certifies that the plan has been amended and appropriate firewalls are in place
  - Exception for certain enrolment functions
Employer vs. Group Health Plan

Under HIPAA an Employer sponsored health plan is an entity separate from the Employer.
## Separation of Information

### Employer

- Management, Supervisors, Other Employees
  - Workers’ Compensation
  - OSHA
  - FMLA
  - All other employee relations issues

- Human Resources Department
  - Life and Accidental Death and Dismemberment Insurance
  - Short-Term Disability
  - Long-Term Disability
  - Voluntary Permanent Life Insurance
  - Dependent Care FSA
  - Automotive and Homeowners Insurance
  - Prepaid Legal
  - Business Travel Accident

### Health Plan

- Health Plan Workforce
  - (Strive to Keep Information Contained)
  - Medical
    - HMOs
    - PPO
    - Wellness
    - Expat plans
  - Prescription Drugs
  - Dental
  - Health Care FSA
  - Vision
  - Employee Assistance Program
  - Health Reimbursement Account
  - Long-Term Care

---

**Not Covered by HIPAA** vs **Covered Entity Under HIPAA**

[Diagram showing the separation of information and the categories of covered and not covered by HIPAA]
Plan Workforce

Health Plan Workforce is responsible for carrying out Plan administrative duties

- Employee Benefits
- Positions within IT that must have access to PHI as part of the job function
- Individuals in charge of benefits at particular facilities
- Plan Committee Members
- Positions within the legal department that must have access to PHI as part of job function
- Privacy Official
- Security Official
Keep PHI Contained

✧ To avoid allegations that PHI is used for hiring and firing decisions
  ■ HIPAA is designed to prevent group health plans from utilizing PHI to create performance issues in order to fire or refuse to hire individuals whose health issues are costly to the Employer
  ■ Keeping PHI contained within the Plan Workforce protects the Employer from these allegations
  ■ This protection is lost once PHI is improperly used or disclosed
When In Doubt

Think about how you learned the information

From employee relations issues like OSHA, FMLA, or Workers’ Compensation?
- Not subject to HIPAA
- Still keep confidential!!!

While providing health care benefits to participants or properly administering the Health Plan?
- Subject to HIPAA
- May not be used for hiring and firing decisions
Recent Changes to HIPAA
Recent Changes to HIPAA

- HHS issued final regulations implementing changes to HIPAA made by the HITECH Act and GINA, effective March 26, 2013.

- HITECH Act (the Health Information Technology for Economic and Clinical Health Act of 2009) broadened HIPAA’s privacy and security provisions.

- GINA (the Genetic Information Nondiscrimination Act) amended HIPAA to govern the use and disclosure of genetic information.

- Many provisions in the final regulations mirror the interim final regulations issued in 2009 and the proposed regulations issued in 2010.
Expansion of Participant Rights

- Individuals can obtain electronic access to their own PHI maintained electronically in a designated record set.
- The final regulations provide that Covered Entities:
  - *Do not* have to purchase a new software system to accommodate these requests.
  - Can provide a hard copy of the information, if the individual rejects available electronic forms.
  - Can charge a reasonable cost-based fee.
- Individuals can also direct the Covered Entity to transmit PHI electronically to a third party.
Expansion of Participant Rights

- The final regulations also changed the timeline within which Covered Entities must respond to an individual’s request for their own PHI when records are off-site
  - The old regulations allowed 60 days, plus a 30-day extension
  - The new regulations allow only 30 days, but retain the 30-day extension
The final regulations prohibit plans from using or disclosing “genetic information” for “underwriting purposes,” which includes:

- Determining eligibility, coverage, and payments
- Negotiating a TPA contract or insurance policy

Effective September 23, 2013, this prohibition applies to all plans subject to the privacy regulations, except issuers of long-term care insurance
Disclosing PHI for Marketing Purposes

- Under HIPAA, Covered Entities must obtain a valid authorization before using or disclosing PHI for marketing purposes.

- The new regulations change the definition of “marketing” to exclude certain communications, including:
  - Certain treatment and health care operations purposes if the Covered Entity does not receive direct or indirect, financial payment from a third-party who is promoting its product or service.
  - Refill reminders or otherwise communicate about a drug currently prescribed to the participant, so long as financial payment is reasonably related to the cost of making the communication.
Selling PHI

♦ Under HIPAA, Covered Entities must obtain a valid authorization before selling PHI, which the prior regulations did not clearly define.

♦ The new regulations define “sale” to mean disclosure of PHI in exchange for an indirect or direct benefit — whether or not the benefit is financial.

♦ There are some exceptions, including exchanging PHI for a benefit for purposes of:
  - Research for reasonable, cost-based fees
  - Treatment
  - Due diligence related to a merger and acquisition of the Covered Entity
  - Meeting legal requirements
Effective September 23, 2013, the final regulations change the definition of a “Breach” of unsecured PHI

- The prior standard focused on harm to the individual
- The new standard presumes the existence of a Breach if PHI is acquired, accessed, used, or disclosed, unless a risk assessment demonstrates a low probability that PHI has been compromised

To perform this risk assessment, Covered Entities must consider:
- The nature and extent of the PHI
- The unauthorized person who received the disclosure
- Whether the PHI was actually acquired or viewed
- The extent to which the risk has been mitigated

Workforce Members and Business Associates who discover a Breach should alert the Plan’s Privacy Official
Breach Notification

♦ Consistent with the former regulations, Covered Entities must provide notice of the Breach to individuals, HHS, and, in some cases, the media.

♦ The new regulations did not change the content of notification requirements, such as:
  ■ Description
  ■ Types of PHI
  ■ Steps individual should take, and
  ■ Contact number for questions
Breach Notification

♦ Covered Entities must provide the Notice to participants and, when warranted, the media within 60 days of the day that the Covered Entity discovered the Breach

♦ Covered Entities also must provide Notice to HHS:
  - Within 60 days of the discovery if the Breach involves 500 or more individuals
  - Within 60 days after the end of the calendar year in which the Breach was discovered if the Breach involves less than 500 individuals
  - Previously, the deadline was the year in which Breaches actually occurred
Notice of Privacy Practices

The Notice of Privacy Practices must reflect additional content, including disclosures of the:

- Breach notification requirements
- The prohibition on using genetic information for underwriting purposes
Notice of Privacy Practices

♦ Covered Entities must redistribute the Notice within 60 days of a material change, which includes adding new content
  ■ Covered Entities must revise their Notices by September 23, 2013 and distribute a new Notice within 60 days of the revision
  ■ A health plan that maintains a website must post the revised Notice on the website by September 23, 2013
  ■ A health plan may distribute the notice in its next Annual Notice Packet so long as the packet is mailed by November 22, 2013
Penalties

♦ Under the final rule, Covered Entities are liable for civil penalties if their “agents” violate HIPAA within the scope of agency

♦ The new regulations clarify that an agent’s status is a fact-specific determination under Federal common law, considering:
  - The time, place, and purpose of the agent’s conduct
  - Whether the conduct was subject to a Covered Entity’s control
  - Whether the conduct is commonly done by a Business Associate
  - Whether or not the conduct in question was reasonably expected
  - The terms of a Business Associate Agreement (if any) and the parties’ ongoing relationship
The Final Regulations also:

- Clarify that photocopiers, facsimiles, and other office machines that retain electronic data are subject to HIPAA’s Privacy and Security Regulations.
- Broaden individual authorizations to facilitate research, disclosure of child immunization proof to schools, and family members access to decedent information.
- Formalize the protection of decedent’s PHI for 50 years after death, but only to the extent that the Covered Entity keeps records of the PHI for that long.
- Formalize the interim final regulations provisions on non-compliance due to willful neglect and penalties.
- Expand the liability and definition of “Business Associates”.
Compliance Deadlines

♦ Most new provisions have a compliance deadline of September 23, 2013

♦ There are a few exceptions
  ■ Annual Enrollment – Post the new Notice of Privacy Practices if a website is maintained with plan information
  ■ November 22, 2013 – Distribute a new Notice of Privacy Practices (only posting on a website is not enough)
  ■ September 23, 2014 – Amend certain Business Associate Agreements in effect as of January 25, 2013
Identifying Business Associates
Identify a Business Associate

Definition of Business Associate expanded by final regulations to include subcontractors

Generally, an entity that performs a function or activity on behalf of a Covered Entity or provides certain specific services for a Covered Entity and has access to PHI such as:

- Claims processing or administration
- Data analysis
- Utilization review
- Quality assurance
- Billing
- Legal
- Actuarial
- Accounting
- Consulting
- Data aggregation
Business Associates

Includes:

- E-prescribing Gateways
- Entities that provide data transmission services to a Covered Entity for PHI and require access to such PHI on a routine basis
- Entities that offer personal health records to individuals on behalf of a Covered Entity
- Subcontractors that create, receive, maintain, or transmit PHI on behalf of a Business Associate such as a mailing vendor hired by a medical plan Administrator to mail EOBs

- Under final rules subcontractors must receive written assurances from their vendors and agents with access to PHI that they will appropriately safeguard PHI
Not a Business Associate

Under the final rules the following are not Business Associates:

- Health care providers, with respect to disclosures by a Covered Entity to the health care provider concerning treatment of the individual
- Plan sponsors, with respect to disclosures by a group health plan (or a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent the plan sponsor has complied with the requirements to receive PHI from a plan
- Government agencies, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes, to the extent those activities are authorized by law
- Workforce members of the Covered Entity
Examples of Plan Business Associates

- **Legal Counsel:** When have access to PHI, such as claims and appeals, notice requirements, billing disputes with providers, and investigation of fraudulent claims or enrollment

- **Actuaries:** When using claims data to determine rating structures and other financial aspects related to plans
  - Actuaries often have access to PHI in the process of examining large claims, providing experience reports, recommending rating structures, and reviewing reinsurance reimbursements

- **Accountants and Outside Auditors:** When have access to claims data when performing plan audits

- **Consultants and Brokers:** If have access to PHI when reviewing a plan’s financial operation, reviewing the performance of other service providers, or providing general advice to the plan administrator
Examples of Plan Business Associates

- **Vendors performing data aggregation**: Data aggregators are Business Associates who create PHI for, or receive PHI from, more than one Covered Entity to permit data analyses that relate to the health care operations of the respective Covered Entities.
  
  *Example*: Vendor that aggregates claims data from medical, prescription and wellness claims for multiple plans.

- **Independent Review Organizations (IROs)**: Health Care Reform added the requirement for external claims review by IROs which will be either a direct Business Associate of a self-insured plan or a subcontractor of the plan’s TPA.

- **IT Vendors and E-mail Providers**: Entities that process or transmit PHI on behalf of Covered Entities are Business Associates if they require access to PHI on a routine basis to perform their functions.
Examples of Plan Business Associates

- COBRA administrator

- **Software vendors** who host software and patient information on its own servers, or accesses patient information when troubleshooting software

- **Printing contractors, mailing houses, and shredding services** if PHI is printed, mailed, or shredded by the entity
Not Business Associates

♦ **Conduits:** entities that transport information but do not access it other than on a random or infrequent basis as may be necessary for the performance of the transportation service, or as required by law

    ▪ Under the Final Regulations the conduit exception is narrow and limited to transmission services such as UPS and FedEx
      
        ➢ An entity that maintains PHI on behalf of a Covered Entity such as an e-mail provider is a Business Associate and not a conduit, even if the entity does not actually view the PHI on a routine or frequent basis

♦ **Janitorial Services:** confidentiality agreement is recommended (still need appropriate physical safeguards)

♦ **Provider/Health Plan Transactions:** when provider discloses PHI to the plan for payment purposes or when provider accepts discounted rate to participate in network
Not Business Associates

- **Workforce members**: employees, volunteers, trainees, and other persons under direct control of a Covered Entity or Business Associate are not Business Associates themselves, regardless of who pays them.

- **Telecommunications Relay Services**: enables telephone communication for hearing or speech impaired; public service.

- **Insurer/HMO**: for a fully insured plan
  - Where the insurer provides administrative services for a self-funded plan, insurer is Business Associate.

  *Example*: Insurer administers health FSA benefits.

- **Stop-Loss Insurer**: if insurance is purchased by the employer (confidentiality agreement is recommended).
HIPAA Enforcement
Recent Developments/Trends

- In the past, a focus on investigation of specific complaints.
- The passage of the HITECH Act drastically changed the privacy and security enforcement landscape:
  - Required audits and investigations by HHS
  - Increased civil penalties
  - Causes of action to state attorney general
Complaints and Investigations

- An individual may file a complaint with the HHS Office of Civil Rights (OCR)
  - Must be within 180 days
  - Anyone can file

- Protections for complainants
  - Cannot retaliate against individuals who believe in good faith that there has been a privacy rule violation and:
    - File complaints
    - Help HHS with the investigation or compliance review
    - Oppose a practice in a reasonable manner
Complaints and Investigations

♦ Enforcement Statistics
  ■ 80,836 privacy complaints filed in the last 10 years
    ➢ Approximately ¼ resulted in enforcement after investigation
  ■ 3,464 new complaints from January to April 2013
♦ Health plans are the fourth most common entities to require corrective action
Compliance Reviews

- OCR has the authority to initiate reviews on its own to determine whether Covered Entities are complying with the Privacy and Security Rules
  - The HITECH Act mandates investigation of complaints and compliance review if possible violation due to “willful neglect”
- No need for a specific complaint
  - Media reports
  - “Large” HITECH breach notifications
- Covered Entities must cooperate with HHS investigation or review
  - Submit reports
  - Access to records and facilities
  - Subpoena power
The HITECH Act requires that HHS conduct compliance audits of Covered Entities and Business Associates.

Pilot program completed in 2012:

- Significant focus on documentation proving compliance.
- Establish framework for future audits:
  - Request documents, site visits, interviews with employees.
  - 169 different modules focusing on privacy, security and Breach notification.
Informal Resolutions

- Violation revealed by either an investigation, compliance review, or an audit
- Before pursuing harsher sanctions, OCR will try to “informally” resolve violation
  - Voluntary compliance
  - Corrective action
  - Resolution agreement
    - Pay a fine and implement corrective action
    - Agreement often published
Civil Penalties

- Covered Entities and Business Associates can be liable
- Opportunity to assert defenses or mitigating factors and request hearing
- Each violation can be for each separate violation that relates to each affected participant

*Example*: An impermissible use or disclosure and a safeguard violation
## Civil Penalties

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
<th>All Violations of an Identical Provision in a Calendar Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect Corrected</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
Criminal Penalties

Criminal penalties for wrongful disclosures of PHI apply to individuals irrespective of whether they are employees.

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowing Violations</td>
<td>Up to $50,000 and 1 year in prison</td>
</tr>
<tr>
<td>False Pretenses</td>
<td>Up to $100,000 and 5 years in prison</td>
</tr>
<tr>
<td>Intent to sell, transfer, or use for commercial advantage, personal gain or malicious harm</td>
<td>$250,000 and/or 10 years in prison</td>
</tr>
</tbody>
</table>
State Attorneys General

- The HITECH Act authorized state attorneys general to bring civil actions in federal court for violations
- $100 per violation, capped at $25,000 for identical violations during a calendar year
Enforcement Examples

- **Alaska Department of Health and Social Services – June 2012**
  - Self-reported a possible Breach involving the theft of a USB drive containing PHI from an employee’s vehicle
  - $1.7 million fine and corrective action plan with new policies regarding handling of ePHI
  - Failures:
    - Perform a risk analysis
    - Implement sufficient risk-management measures
    - Provide security training for its employees
    - Implement device and media controls
    - Properly encrypt media devices
Enforcement Examples

Massachusetts Eye and Ear Associates Inc. – September 2012

- Self-reported Breach involving the theft of an unencrypted laptop containing PHI of 3,500 patients in South Korea
  - Computer was password protected
  - Equipped with an internet tracking device that reported that the OS had been reinstalled without the needed software to access the PHI
  - Hard drive remotely disabled

- What happened?
Reporting a Breach to HHS
The HITECH Act requires Covered Entities to report all Breaches of Unsecured PHI to HHS

- HHS is required to report the number and nature of these Breaches to Congress annually.
Reporting a Breach of Unsecured PHI to HHS

- Over 600 Breach incidents affecting 500 or more individuals are listed on the HHS OCR website
  - Most involve theft or loss of laptops or other portable electronic devices
  - Other Examples:
    - Explanation of benefits mailed to unauthorized individuals
    - Third party hacking into Covered Entity's network
    - Improper disposal of PHI in a public area
Reporting a Breach of Unsecured PHI to HHS

- Breaches are reported online through the HHS OCR website
Reporting a Breach of Unsecured PHI to HHS

Notice to the Secretary of HHS of Breach of Unsecured Protected Health Information

<table>
<thead>
<tr>
<th>Breach Affecting</th>
<th>Report Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ 500 or More Individuals ☐ Less Than 500 Individuals</td>
<td>☐ Initial Breach Report ☐ Addendum to Previous Report</td>
</tr>
</tbody>
</table>

**Section 1 - Covered Entity**

<table>
<thead>
<tr>
<th>Name of Covered Entity:</th>
<th>Contact Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address:</td>
<td>Contact Phone Number:</td>
</tr>
<tr>
<td>City:</td>
<td>Contact E-mail:</td>
</tr>
<tr>
<td>State: AL</td>
<td>Zipcode:</td>
</tr>
<tr>
<td></td>
<td>Type of Covered Entity:</td>
</tr>
</tbody>
</table>


# Reporting a Breach of Unsecured PHI to HHS

## Section 2 - Business Associate

*Complete this section if breach occurred at or by a Business Associate*

<table>
<thead>
<tr>
<th>Name of Business Associate:</th>
<th>Business Associate Contact Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address:</td>
<td>Business Associate Contact Phone Number:</td>
</tr>
<tr>
<td></td>
<td>XXXX-XXXX-XXXX</td>
</tr>
<tr>
<td>City:</td>
<td>Business Associate Contact E-mail:</td>
</tr>
<tr>
<td>State: AL  Zipcode:</td>
<td></td>
</tr>
</tbody>
</table>

---

---

---
# Reporting a Breach of Unsecured PHI to HHS

## Section 3 - Breach

### Date(s) of Breach:

MM/DD/YYYY (- MM/DD/YYYY)

### Date(s) of Discovery:

MM/DD/YYYY (- MM/DD/YYYY)

### Approximate Number of Individuals Affected by the Breach:


### Type of Breach:

- Theft
- Loss
- Improper Disposal
- Unauthorized Access/Disclosure
- Hacking/IT Incident
- Unknown
- Other

### Type of Breach (Other):


### Location of Breached Information:

Please select the location of the information at the time of the breach. If breach type is "Other", please describe the location of the information in more detail in the Description section below.

- Laptop
- Desktop Computer
- Network Server
- E-mail
- Other Portable Electronic Device
- Other

---

Mazursky Constantine LLC
Reporting a Breach of Unsecured PHI to HHS

Type of Protected Health Information Involved in the Breach:
- Demographic Information
- Financial Information
- Clinical Information
- Other

Brief Description of the Breach:
Please include the location of the breach, a description of how the breach occurred, and any additional information regarding the type of breach, type of media, and type of protected health information involved in the breach.

Safeguards in Place Prior to Breach:
- Firewalls
- Packet Filtering (router-based)
- Secure Browser Sessions
- Strong Authentication
- Encrypted Wireless
- Physical Security
Reporting a Breach of Unsecured PHI to HHS

Section 4 - Notice of Breach and Actions Taken

Date(s) Individual Notice Provided: MM/DD/YYYY - MM/DD/YYYY

Was Substitute Notice Required? Yes No

Was Media Notice Required? Yes No

Actions Taken in Response to Breach:
Please select the actions taken to respond to the breach. If selecting the "Other" category, please describe the actions taken in the section below.

Security and/or Privacy Safeguards
Mitigation
Sanctions
Policies and Procedures
Other

Describe Other Actions Taken:
Please describe in detail any actions taken following the breach in addition to those selected above.
Reporting a Breach of Unsecured PHI to HHS

Section 5 - Attestation

Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at 45 C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided on this form will be made publicly available by posting on the HHS web site pursuant to § 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to § 13402(i) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

I attest, to the best of my knowledge, that the above information is accurate.

Name: ___________________________ Date: ________________

Typing your name represents your signature

MM/DD/YYYY

Submit
Frequently Asked Questions
FAQS

♦ Whether enrollment information is considered PHI?
  ■ Depends on the type of information, and
  ■ Whether the information is in the hands of the employer or the plan
    ➢ Hands of the employer when performing enrollment
    ➢ Hands of the plan when provided to a Business Associate to perform a service for the plan
FAQS

- Whether a plan can disclose PHI in cases of suspected prescription drug misuse
  - Depends on why the disclosure is being made (e.g., prevent fraud and abuse, treatment of the suspected prescription abuse), and
  - To whom the disclosure is being made (e.g., the employer, providers, or law enforcement)
    - May always put protections in place without disclosing PHI (e.g., limiting the pharmacy locations where the participant may fill prescriptions)
FAQS

♦ Whether Business Associate Agreements are required with service providers who may have inadvertent contact with the PHI?

- Not required if the work performed by the service provider does not involve the use or disclosure of PHI and any disclosure that does occur is incidental and limited in frequency

- Nonetheless, plans can face liability when PHI is entrusted to any third party, regardless of whether the third party is a Business Associate

- Plans still need to protect themselves by safeguarding PHI (e.g., locking filing cabinets, shredding paper documents containing PHI, etc.)
FAQS

♦ Whether a plan may direct TPAs to share PHI with one another?
  ■ Permissible provided proper Business Associate agreements are in place
  ■ TPAs often require nondisclosure agreements
FAQS

♦ Whether the plan may use e-mail to discuss PHI with participants?

- Safeguards must be applied to reasonably protect privacy (e.g., checking the e-mail address for accuracy)

- Transmission of electronic PHI must comply with the Security Rule

- May respond to participant initiated communications from personal e-mail
  - Best practice is to send an e-mail explaining that communications via personal e-mail are not secure and
  - Confirm with the participant that it is okay to respond using the personal e-mail
Whether Health FSAs are subject to the HIPAA Privacy and Security rules?

- Health FSAs are considered group health plans subject to the HIPAA Privacy and Security Rules
  - *Exception:* Health FSAs with fewer than 50 participants that are administered by employers
- Fully-insured “hands-off” approach is not available
Whether the HIPAA Notice of Privacy Practices may be distributed electronically?

- Very limited situations where the recipient has agreed to receive the notice electronically (and not withdrawn that agreement)
- A paper notice must be provided:
  - Upon request, and
  - If the plan knows the electronic transmission failed