HIPAA Privacy Resource Manual

A Guide to HIPAA Privacy Awareness

Department of Human Resource Management

Office of Health Benefits Programs

This manual is for guidance and reference purposes only. It is of a general informational and educational nature. While care has been taken to ensure the accuracy of the information contained in this manual, The Office of Health Benefits Programs assumes no liability with regard to any errors that may be contained herein. This information provided is not intended to replace, nor should it be construed as replacing, professional legal advice.

About This Resource Manual

Beginning April 14, 2003, health plans will be required to comply with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. These new federal regulations impose standards for safeguarding personal individually identifiable medical information, also referred to as "protected health information (PHI)." The Rule creates significant requirements and limitations in the way that PHI is handled within the Office of Health Benefits Programs, the State Agency and Local Employer's Benefits Offices and shared with those outside the Plan.

How to Use This Resource Manual

This manual is a supplement to HIPAA Privacy Awareness Training. It summarizes important information about the privacy rules and provides tools to ensure the Office Of Health Benefits Programs meets its HIPAA compliance objectives.

HIPAA Privacy Awareness Training

To facilitate your understanding of the HIPAA Privacy Rule and how it affects your organization, you should review the accompanying, self-study training presentation entitled "HIPAA Privacy, Confidentiality and You"

The Privacy Training presentation is designed to provide you with a comprehensive summary of the HIPAA Privacy Rule and your role for ensuring compliance, and includes a Quick Refresher to test your knowledge of the covered subject matter.

Table of Contents

HIPAA Overview

HIPAA is an abbreviation for Health Insurance Portability and Accountability Act of 1996. Two of HIPAA's main goals are to:

- Make health insurance more portable when persons changed employers, and
- Make the health care system more accountable for costs and try to reduce waste and fraud.

HIPAA has four associated regulations or "rules":

- Standardized formats for all electronic data (computer-to-computer) information exchanges (the "transactions standard")
- Standardized "identifiers" for health providers and health plans
- Information system security standards
- Privacy standards also referred to as the "HIPAA Privacy Rule"

The manual and the accompanying presentation focus on the HIPAA Privacy Rule.

What is the HIPAA Privacy Rule?

The HIPAA Privacy Rule applies to individually identifiable health information created or maintained by health care providers, health plans, and health care clearinghouses ("Covered Entities"). This information is also referred to as protected health information (PHI). The Department of Health and Human Services (HHS) issued the regulations. The Office for Civil Rights (OCR) is the HHS department responsible for implementing and enforcing the Privacy Rule.

The Privacy Rule is the first comprehensive federal protection implemented to safeguard private health information. The Rule creates national standards to protect the medical records and other personal health information of individuals.

Specifically, the Privacy Rule was enacted to:

- Set boundaries on how an employee's personal health records are used or disclosed to others
- Establish protocols or safeguards that Covered Entities must follow to protect private health information
- Restrict employers from using PHI in employment decisions (particularly against employees, such as in hiring/firing or promotion decisions)
- Hold violators accountable with civil and criminal penalties
- Give employees more control over their own personal health information
    - Employees must be notified about how their private health information may be used or disclosed, and in many cases, have the right to object to certain disclosures
    - Release of private health information about employees is generally limited to the minimum necessary for the situation or purpose of the disclosure
    - Employees can examine and obtain a copy of their own health records and request corrections

The Privacy Rule limits how PHI is shared, prevents employers from using PHI in employment decisions, and requires employers to establish and document safeguards for handling PHI.

When is the Privacy Rule effective?

The effective date for most Covered Entities is April 14, 2003.

What if a state has its own set of privacy regulations?

The HIPAA Privacy Rule is intended to provide a federal safety net for personal medical information. State laws that provide stronger privacy protection will continue to apply over and above the new federal privacy standards.

What needs to be done to comply with the Privacy Rule?

Specifically, the Health Plan will have to:

- Provide a notice to all individuals whose protected health information (PHI) will be used or disclosed. This notice will describe their privacy rights and how PHI may be used or disclosed
- Develop and implement privacy policies and procedures to safeguard the PHI they maintain or are able to access
- Designate a Privacy Officer who will be responsible for ensuring the Privacy Rule is followed, and who will be a resource for others should you have questions about the privacy policies or procedures
- Amend plan documents for HIPAA's Privacy Rule
- Provide training materials for employees on the new privacy policies and procedures
- Ensure that the "Business Associates" have compliant policies and procedures in place
- Establish appropriate safeguards to protect the privacy of PHI, including:
    - Administrative safeguards, such as procedures for the monitoring of the internal flow of PHI and enforcement of complaint and discipline policies
    - Technical safeguards, such as computer firewalls
    - Physical safeguards, such as locking doors and filing cabinets and restricting access to certain spaces

The Office of Health Benefits Programs' HIPAA Privacy Rule Compliance Program

Privacy Officer

The Office of Health Benefits Programs' Privacy Officer is responsible for implementing and overseeing privacy-related policies and procedures, and adherence to the compliance standards for safeguarding protected health information (PHI) for the Plan. Please refer to the Office of Health Benefits Programs' Privacy Policies and Procedures Manual for more detailed information.

Employee Privacy Notice

HIPAA requires Covered Entities, such as your health plan, to provide employees and plan participants with a "notice of privacy rights" no later than April 14, 2003. The notice must describe, in general terms, how we will protect health information, and specify the individuals' right to:

- Obtain a copy of their own PHI
- Correct errors in their PHI
- Get an accounting of how their PHI has been used and to whom it has been disclosed
- Request limits on access to their own PHI
- Complain and seek relief if they believe their own PHI has been mishandled

As required by HIPAA, this notice is to be distributed to all current employees and plan participants by April 14, 2003. For new hires and new plan participants, the notice should be provided no later than 60 days after hire. The Notice also needs to be redistributed if it changes materially, or once every three years, whichever is sooner.

Amended Plan Documents

Generally, to have access to PHI, other than enrollment/dis-enrollment information from a health plans, HIPAA requires an amendment to the applicable plan documents to describe the privacy policies and procedures and limit use and disclosure of PHI to the "minimum necessary." The amended plan documents should include the following policies and procedures the Plan has adopted for:

- An individual's access to his or her own PHI
- Amendments and correction of PHI
- Requested restrictions on use and disclosure of PHI
- Filtering the "minimum necessary" information when using or disclosing PHI for non-treatment purposes
- Record keeping and record retention
- Business associates' breach of contractual privacy provisions
- Sanctions and corrections of privacy violation

Protected Health Information (PHI)

What is Protected Health Information (PHI)?

PHI is health information about a person created or received by a health plan, other covered entity, or by an employer that contains data that identifies an individual or could reasonably be used to identify an individual. The person could be living or dead. This information must be about the past, present or future physical or mental health of a person, or the payment of health care for that individual. The information could be in any form – written on paper, displayed or stored in a computer, or spoken in conversation. PHI could include a person's name or other information that when combined, identifies the person. The identifying data could be one or any combination of:

- Name
- Date of birth
- Gender
- Medical records number
- Health plan beneficiary numbers
- Address, zip code
- Phone number, email address, fax number, IP address
- License numbers
- Full face photographic images
- Social Security number

PHI identifies people very specifically; can be electronic, paper or verbal; and must relate to a person's health condition, care, or payment for care.

What are examples of PHI?

Examples of PHI include:

- Individual medical records – (becomes PHI only if the information is received by the health plan)
- Medical bills from the hospital, diagnostic information, other
- Doctor/patient information that is part of the health plan record
- Emails – electronic conversations or discussions about an employee's health or medical condition
- Other electronic files – stored information about employees that may include individually identifiable health information (i.e., claims utilization data, stop-loss coverage reports, etc.)
- Personal written notes or files – from conversations with employees or others about an employees' health or medical condition, or those of other plan participants (i.e., employees' covered dependents)

The Privacy Rule limits how entities may share and use PHI, so it's important to recognize PHI when you see it and follow procedures for safeguarding it.

What kind of health information is excluded from PHI?

Information normally maintained in personnel files for employment purposes is not considered PHI. This includes information used to process:

- FMLA or sick leave requests
- Substance abuse screening results
- Pre-employment physicals or fitness for duty results
- Workers' Compensation claims
- Disability Plan claims, ADA accommodations or disability retirements

Important Note: PHI should not be combined with the health information that's normally kept in your personnel files. It should be kept totally separate. And PHI that's kept separate from your personnel files should not be used to make employment decisions or to address absenteeism issues.

Generally, "employment records" are not considered PHI. And, PHI records should be kept totally separate from employment records.

What is meant by "Use" and "Disclosure" of PHI?

The Privacy Rule limits both the *use* and *disclosure* of PHI. "Use" refers to what the Plan does with PHI inside their organization. "Disclosure" means that PHI is given out to an external entity for use. Generally, employees can authorize for PHI to be disclosed to external entities, or to object to such disclosure. But, in some instances, authorization is required and disclosure is governed by law.

Employees or plan participants can always request their own information or authorize release of their PHI to others on their behalf.

Written, employee authorization is required for any use or disclosure not specifically permitted or required by the Privacy Rule.

When is disclosure of PHI permitted?

This chart summarizes the individual control health plan participants have on the disclosure of their own PHI.

Employee Control	Description of Permissible Use or Disclosure
No Consent or Authorization Required	• To or by Health Plan or Health Care Clearinghouse for Treatment, Payment or Health Care Operations ("TPO") • To or by Business Associate for TPO according to HIPAA privacy agreement • To or by Plan Sponsor for TPO according to terms of health plan document
Authorization Required	Uses or disclosures other than for TPO
Opportunity to Agree or Object to Disclosure	• Facility directories • Disaster relief • To persons involved with an individual's care (family member)
No Authorization Required and No Opportunity to Agree or Object	• Public health activities • Workers' Compensation • Judicial proceedings • Law enforcement • Special government functions • Notify family members or personal representative of a person's death • Research • About victims of abuse or domestic violence • Health oversight activities • Certain organ, eye, or tissue donation • To avert serious threat to health or safety

What is an "authorization"?

An "authorization" is defined as an individual's specific and detailed grant of permission to a health plan or other Covered Entity to disclose the individual's protected health information. Health plans must generally obtain a written authorization from an individual for any use or disclosure of PHI other than for TPO (i.e. "routine purposes").

A health plan may make enrollment in the health plan or eligibility for benefits conditional on the employee providing an authorization to enrollment. However, the health plan cannot make enrollment or benefits conditional on the receipt of an authorization to use PHI for non-routine purposes.

To be valid, an employee authorization must specifically:

- Describe the information to be used or disclosed
- State the person or entity to which the information is to be released *and* how the PHI will be used
- State the expiration date or event that will terminate the authorization (i.e., end of plan year for a plan enrollment authorization)
- State the individual's right to revoke the authorization
- Expressly acknowledge that the information may be subject to re-disclosure by the recipient
- Be signed and dated by the employee or plan participant

You can use or disclose information without an employee authorization for:
***Treatment* – for example, if an employee is unconscious, PHI can be provided to a doctor for treatment purposes**
***Payment* – to ensure that claims for health care treatment are paid according to plan terms**
***Health Plan Operations* – to make sure health plans operate efficiently (PHI may be used or disclosed for such things as quality assessments, audits, actuarial studies, fraud/abuse detection, underwriting, and premium ratings)**

When is an authorization necessary?

No authorization is required from an employee or plan participant to use or disclose information for routine purposes, like treatment or payment, or for core health plan operations. However, employees or plan participants must sign an authorization before information can be used for other purposes like certain kinds of marketing and fundraising, or for an employer to use PHI in an employment decision.

When can employees object to use or disclosure of PHI?

In some cases, employees or plan participants have the opportunity to agree or object to disclosure of their PHI. For example, employees may request that certain "normally permitted" uses and disclosures be restricted, such as disclosure for treatment or payment operations (TPO). For this type of objection to be valid, employees must provide a written objection stating how they wish the disclosure to be limited or restricted.

In some cases, employees may be asked to agree or object, including a verbal conversation. For example, employees may object to a disclosure to someone involved in their care, such a family member.

Authorization is not required, and there is no opportunity to object in certain emergency situations. However, employees can object to having their PHI used to help disaster relief efforts. Employees can also request that their name or other identifying information not be included in hospital directories, or on other lists maintained by health care providers.

Sometimes, there is no opportunity for employees to agree or object to disclosures, such as when PHI is needed for Workers' Compensation purposes, when subpoenaed in a lawsuit, to avert a serious threat to health or safety, and other situations specified by the Privacy Rule.

What is meant by "minimum necessary"?

The Privacy Rule requires that a health plan make reasonable efforts to limit the use or disclosure of information to that which is the "minimum necessary" to accomplish the intended purpose. The "minimum necessary" limitation does not apply to:

- Disclosures to a health care provider
- Uses or disclosures made to the individual who is the subject of the PHI
- Certain disclosures to the Secretary of HHS
- Other uses or disclosures required by applicable law

Minimum necessary means that you only disclose the specific PHI that is necessary to satisfy a particular need or request.

Covered Entities

Almost every organization that provides or pays for health services, or exchanges health data of any kind, is within the reach of the HIPAA Privacy Rule. The Privacy Rule specifies that health plans, health care providers, and health care clearinghouses are "Covered Entities." Employers are not specifically mentioned as a Covered Entity. However, employers must also address the effect of HIPAA on human resource operations to ensure PHI is safeguarded.

Employers who act as health plan providers, such as those who sponsor on-site medical clinics or facilities, are also covered, and may have broader responsibilities for safeguarding PHI under the Privacy Rule.

Which health plans are covered?

Medical	Medicare (Parts A & B)
Dental	Medicare + Choice
Vision	Health Insurance Issuers
Prescription Drug	Multiple Employer Health Plans
Mental Health	HMOs

Health Care Flexible Spending Account (FSA)

Other Government Funded Health Plans

Issuers of Long-Term Care Policies (excluding Nursing Home/Fixed Indemnity Policies)

Which health plans are not covered?

- Disability Plans
- Life Insurance
- Workers' Compensation
- Health Plans that have less than 50 participants and are not administered by someone other than the plan sponsor.

Business Associates

By law, the Privacy Rule applies only to the health plan as a "covered entity". However, the external vendors the Plan uses to assist with the maintenance and administration of the plan, and with whom the Plan shares PHI, are referred to as "Business Associates." This means that in order to share PHI with the Business Associates, the Plan must obtain satisfactory written assurances from them that they have the necessary protocols in place to safeguard the PHI of the employees and other plan participants. Also, PHI must only be given to the Business Associates to help them carry out the administrative and other functions that have been contracted for, and not for their own independent use (such as mailing lists for other purposes).

What constitutes a Business Associate relationship?

A Business Associate relationship exists when an individual or entity, acting on behalf of the health plan, assists in performing a function involving the use or disclosure of PHI subject to HIPAA regulations. Such functions include:

- Claims processing or administration
- Data analysis, processing or administration
- Utilization review
- Quality assurance
- Billing
- Benefit management, practice management, and re-pricing

The Privacy Rule also specifies that providers of legal, actuarial, accounting, data aggregation, management, administrative, accreditation, and financial services are Business Associates if they receive PHI in the course of performing their duties.
Company employees are not considered Business Associates.

Business Associate Agreements

To comply with HIPAA OHB must have Business Associate agreements in place with the health plan's vendors that:

- Establish the permitted uses and disclosures of PHI by the Business Associate. A Business Associate is permitted to use the information for its own proper management and administration.

- State that the Business Associate will refrain from using or disclosing the PHI other than as permitted by the contract or as required by law. Restrictions include:
    - Use appropriate safeguards to prevent use or disclosure of the information other than as provided for in the contract, and report any use or disclosure not provided for in the contract
    - Ensure that agents and subcontractors that receive PHI from the Business Associate agree to the same restrictions and conditions that apply to the Business Associate
    - Provide PHI in accordance with the individual's right to access, inspect, and copy their health information (some exceptions may apply)
    - Provide PHI in accordance with the individual's right to have the Covered Entity make amendments to PHI about them in a designated record set (some exceptions may apply)
    - Provide information required to make an accounting of disclosures of PHI, where such disclosures were made for purposes not related to treatment, payment, and healthcare operations (some exceptions may apply)
    - Return and destroy all PHI in any form at the termination of the contract, where feasible
    - In the event of a material breach of the Business Associate's obligations, the contract must authorize termination

OHB's health plan vendors should have separate health information confidentiality agreements with their own external vendors with whom they share PHI.

Tracking and Recordkeeping

What are the tracking requirements?

Except for uses or disclosures for TPO, the HIPAA Privacy Rule generally provides that disclosure of PHI be tracked and accounted for, and that upon request, employees be informed of how their PHI is disclosed. Employees or plan participants may review and copy their PHI, including information about eligibility, billing, claims, and appeals. Employees must submit their request in writing and forward to the Plan's Privacy Officer. The Plan may charge a reasonable fee for copies. After reviewing their PHI, employees or plan participants can request that their PHI be amended if it is incorrect. The employee's request must be in writing and must provide specific information regarding the correction. This includes source and description of correct information, dates, and key facts. The request may only cover information from the previous six years. If appropriate, the request may be denied (for example, if the employee wants to amend PHI that is complete and accurate).
The entity must respond to the request within 60 days unless an extension is permitted.

Employees have a right to inspect, receive copies of their PHI and request that incorrect PHI be changed. Employees can also request an accounting of certain disclosures.

What are the record keeping requirements?

Covered Entities are required to retain a broad range of documentation regarding their compliance with the Privacy Rule, including:

- Non-routine uses and disclosures of PHI, including specific details on what information was disclosed, where it came from, who received the information, and why it was disclosed
- Authorizations signed by employees or plan participants
- Employee or participants' request for access to or amendment of PHI disclosures
- Employee or participant's request for an accounting of PHI disclosures, except for:
    - Disclosures for treatment, payment, or other health plan operations
    - Disclosures made directly to the employee or plan participant

Generally, the required retention period for documentation is six years from the date of its creation, or the date the documentation was last in effect, whichever is later; but not earlier than April 14, 2003.

If state laws require longer retention of these or any other records held by a Covered Entity, the state requirements control.

Written policies and procedures implemented to safeguard PHI and the Privacy Notice provided to employees and plan participants must also be documented.

What if an employee complains that PHI is mishandled?

HIPAA requires that Covered Entities have an internal process for receiving and evaluating complaints of HIPAA violations. Typically, these complaints will be the responsibility of the Privacy Officer. Individuals who believe that a Covered Entity is not complying with HIPAA requirements may also file a complaint with the Secretary of HHS. Currently the Office of Civil Rights (OCR) within HHS has been designated to receive such complaints. Complaints to HHS must:

- Be filed in writing, either on paper or electronically
- Name the entity that is the subject of the complaint, and describe the acts or omissions believed to violate the HIPAA Privacy Rule
- Be filed within 180 days of when the complaining person knew, or reasonably should have known,
- that the violation occurred (though the Secretary may waive this time limit for "good cause")

If HHS launches an investigation, the Secretary of HHS must notify the Company and any complainants in writing.

The HIPAA regulations direct the Secretary to attempt to resolve problems by informal means, whenever possible. If informal resolution is not possible, the Secretary must issue formal, written findings, which presumably would raise the possibility of further investigation, and legal or financial sanctions.

A Covered Entity may not require individuals to waive their rights to file a complaint as a condition of the provision of treatment, payment, or enrollment in a health plan or eligibility for benefits. Nor may it intimidate or retaliate against complainants.

Employees or participants who feel that their rights have been violated may file a complaint in writing. The Privacy Rule states that employees may not be retaliated against for filing a complaint.

Penalties for Non-Compliance

HHS has broad authority to investigate complaints, conduct compliance reviews, and obtain access to records. HHS has generally delegated the civil enforcement, implementation, and interpretation authority under the Privacy Rule to the Office for Civil Rights. Failure to comply with the HIPAA Privacy Rule means that the covered entity could face a variety of civil and criminal penalties depending on the severity of the offense:

- Health plans are subject to civil penalties of up to $100 per person per plan violation; and up to $25,000 per person, per calendar year for each requirement or prohibition violated.
- If a health plan knowingly violates the HIPAA Privacy Rule by wrongfully obtaining or disclosing PHI, the health plan, or individuals, upon conviction, could be charged by the Department of Justice with a $50,000 fine, up to one year in prison, or both.
- If PHI is obtained or disclosed under false pretenses, the penalties can include a fine of up to $100,000, up to five years in prison, or both

If PHI is obtained or disclosed with the intent to sell, transfer or use it for commercial advantage, personal gain, or malicious harm, the penalties can be as high as a $250,000 fine, up to 10 years in prison, or both.

Training

What are the HIPAA training requirements?

HIPAA's Privacy Rule states that entities must provide and document HIPAA training for employees whose jobs are affected by the Privacy Rule.

What kind of training do I need?

Depending on your job responsibilities, you will need to complete the HIPAA Privacy Awareness Training.

Will we ever need retraining?

If there are changes to the HIPAA Privacy Rule that result in new policies and procedures, you will need to undergo additional training. You also may be asked to participate in a periodic refresher training. Additionally, retraining will be provided to employees whose job activities are affected by a material change in the policies or procedures.

Important Terms to Know

Administrative Services Only (ASO)
An arrangement whereby a self-insured entity contracts with a Third Party Administrator (TPA) to administer a health plan.

Business Associate
A person or organization that performs a function or activity on behalf of a Covered Entity, but is not part of the Covered Entity's workforce. Under certain circumstances, a Covered Entity could also be a Business Associate.

Compliance or Effective Date
Under HIPAA, this is the date by which a Covered Entity must comply with a standard, an implementation specification, or a modification. This is usually 24 months after the effective date of the associated final rule for most entities, but 36 months after the effective data for small health plans. For future changes in the standards, the compliance date would be at least 180 days after the effective date, but can be longer for small health plans and for complex changes.

Covered Entity
HIPAA's regulations directly cover three basic groups: health plans, health care providers, and health care clearinghouses.

Electronic Data Interchange (EDI)
Refers to the exchange of routine business transactions from one computer to another in a standard format, using standard communications protocols.

Group Health Plan
A plan that provides health care coverage to employees, former employees, and their dependents, and is sponsored by an employer.

Health Care Clearinghouse
A public or private entity that is or performs any of the following, including but not limited to:

- Billing services
- Repricing companies
- Community health management information systems or community health information systems, and
- "Value-added" networks and switches are health care clearinghouses if they perform these functions: 1) Processes or facilitates the processing of information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction compliant with EDI; 2) Receives an EDI standard transaction from another entity and processes or facilitates the processing of information into nonstandard format or nonstandard data content for a receiving entity.

Health Insurance Portability and Accountability Act of 1996
A Federal law that allows eligible individuals to qualify immediately for comparable health insurance coverage when they change their employment relationships. Title II, Subtitle F, of HIPAA also gives HHS the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable health care information. Also known as the Kennedy-Kassebaum Bill, the Kassebaum-Kennedy Bill, K2, or Public Law 104-191.

Health Plan
An entity that assumes the risk of paying for medical treatments (e.g., self-insured employer, payer, insurance carrier or HMO) funded by employer or employee organization contributions, employee contributions or both.

Plan Sponsor
An entity that sponsors a health plan. This can be an employer, a union, or some other entity.

Protected Health Information (PHI)
Individually identifiable health information transmitted or maintained in any form or medium, which is held by a Covered Entity or its Business Associate and:

- Identifies the individual or offers a reasonable basis for identification
- Is created or received by a Covered Entity or an employer
- Relates to a past, present, or future physical or mental condition, provision of health care, or payment for health care

Self-Insured
An individual or organization that assumes the financial risk of paying for health care.

Small Health Plan
Under HIPAA, this is a health plan with annual receipts of $5 million or less.

Third Party Administrator
Business associate that performs claims administration and related business functions for a self-insured entity.

Workforce
Under HIPAA, this means employees, volunteers, trainees, and other persons under the direct control of a Covered Entity, whether or not the Covered Entity pays them.

Appendix

Practical Tips for Safeguarding PHI

Training Evaluation Form

Acknowledgement of Training Form

HIPAA Privacy Awareness Training Presentation

Practical Tips for Safeguarding PHI

Oral communication

- Speak quietly when discussing an employee's PHI in public areas
- Avoid the use of names or other identifying information in conversations whenever possible
- Designate "quiet areas" for PHI exchange (i.e., in private office or conference room with door closed)

Telephone use

- Conversations regarding PHI should be conducted where they cannot be overheard, if at all possible (i.e., in private offices or conference rooms with door closed)
- The other person's identity should be confirmed
- Only names and callback numbers should be left on answering machines and voicemail systems if a called party cannot be reached
- Sensitive information should never be left on the answering machine or voicemail device

Copying and printing

- Sensitive information should not be sent to remote printers or photocopiers where access is uncontrolled and the sender is not present to keep track of the output

- Do not dispose of PHI in open wastebaskets or recycle containers; instead shred or otherwise destroy before discarding

Fax use

Facsimile (fax) use is not considered an "electronic transmission" under HIPAA and the Privacy Rule does not address facsimile transmission directly. Still, faxing practices for PHI must be compatible with the HIPAA privacy regulations. Tips include:

- Place the fax machine(s) you will use to transmit PHI in a secure location (or be sure that someone designated to handle PHI is present during the fax transmission to ensure PHI is secure during transmission)
- Do not send PHI to unattended fax machines, or where the physical security of the receiving system is unknown
- Send faxes about PHI only to known locations, where the physical security and monitoring practices of the receiving fax machine are known
- Rely on preprogrammed (and tested) fax numbers set on the sending machine, to reduce dialing errors
- Include a "confidentiality request" that information sent to an incorrect destination be destroyed, and requesting notification to the sender of such errors

Email

- Avoid using email for exchange of PHI; however, HIPAA does not ban the practice. It is safer to convey information over the phone than via unencrypted email

If electronic mail is used to disclose PHI, with copies of the messages should be kept as part of the records retention process

De-Identifying Individual Health Information

Information may be released to external entities that relates to individual employees or plan participants if all of the following are removed, as applicable:

- Name
- Geographic subdivisions smaller than a state
- Dates (except year) of:
    - Birth
    - Admission
    - Discharge
    - Death
- Telephone number
- Fax number
- Email address
- Social Security number
- Medical records number
- Health plan beneficiary numbers
- Account numbers
- License and certification numbers
- Vehicle identification numbers (such as license plate number)
- Device identifiers (such as serial numbers)
- URLs (web “universal resource locators”)
- Internet Protocol (IP) address
- Biometric identifiers (such as finger and voice prints)
- Full face photographic images (and any company images)
- Other unique identifiers

Training Certification Form

To: Human Resources Department

From: _____(Employee Name)

_____(Dept/Work Location)

Subject: Completion of HIPAA Privacy Awareness Training

This is to certify that I completed the HIPAA Privacy Awareness Training.

The training session I attended was:

Group Presentation on _____

Self-study course completed on _____.

_____

Employee Signature Date