HIPAA Privacy

Definitions

Business Associate: A person or company that acts **on behalf of** a covered entity performing functions that involve the use or disclosure of PHI for claims processing, billing, quality assurance, etc. Members of a covered entity's **work force are not** business associates.

Covered entity: All health plans, all health care clearinghouses, any health care provider who transmits health information in electronic form in connection with a covered electronic transaction.

Designated record set: (DRS) is a record that contains information utilized and maintained for the purpose of making decisions about an individual's health care.

Electronic protected health information: (EPHI) means individually identifiable health information that is transmitted, maintained or stored in electronic form.

Genetic information: Subject to this definition, with respect to an individual, information about:

(i) The individual's genetic tests;

(ii) The genetic tests of family members of the individual;

(iii) The manifestation of a disease or disorder in family members of such individual; or

(iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.

Privacy: A scalable set of standards governing the patient's rights over the use and disclosure of their own protected health information (PHI).

Protected health information: (PHI) means individually identifiable health information maintained or stored in electronic or any other form or medium. It includes medical, demographic, and financial information about the patient.

Security: Specific measures a health care entity must take to protect ePHI from unauthorized breaches of privacy, or loss of integrity. It is scalable, flexible, and generally addressable.

Subcontractor: a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

Transactions: The electronic transmission of information between two parties to carry out financial or administrative activities related to health care.

HIPAA Privacy Compliance Officer Responsibilities

This person serves as the focal point for Compliance activities and with regard to planning, implementing, and monitoring the HIPAA PRIVACY Compliance Program.

Compliance to HIPAA Privacy policies is one of the many responsibilities this person has in the office. The HIPAA Privacy Compliance Officer has authority to direct supervised personnel in the office as to the proper procedures to enable compliance with HIPAA Privacy policies. The HIPAA Privacy Compliance Officer has direct access to management.

THE HIPAA PRIVACY COMPLIANCE OFFICER IS RESPONSIBLE FOR THE FOLLOWING:

- **Overseeing and monitoring** the implementation of our HIPAA Privacy Compliance Program.
- **Reporting to management** on a regular basis regarding the progress of implementation, and assisting management in establishing methods to improve the practice's efficiency and quality of services, and to reduce our vulnerability to possible misuse of PHI.
- **Developing, coordinating, and participating in a multifaceted educational training program** that focuses on the elements of the Privacy Compliance Program, and seeks to ensure that all appropriate employees and management are knowledgeable of, and comply with, pertinent federal standards.
- **Ensuring that independent contractors and agents** who furnish medical services to the clinic **are aware of the requirements** of the Privacy Compliance Program with respect to HIPAA and the protection of PHI.
- **Assisting financial management** in coordinating internal Privacy Compliance review and monitoring activities, including annual or periodic reviews of the practice.
- **Independently investigating** and acting on matters related to Privacy Compliance, including the flexibility to design and coordinate internal investigations (e.g. responding to reports of problems or suspected violations) and any resulting corrective action with all employees, providers and sub-providers, agents and, if appropriate, independent contractors.
- **Developing policies and programs** that encourage managers and employees to report suspected improprieties without fear of retaliation.

The HIPAA Privacy Compliance Officer has the authority to review all documents and other information that are relevant to Privacy Compliance activities. These include, but are not limited to, patient records, billing records, and records concerning the marketing efforts of the clinic and the clinic's arrangements with other parties, including employees, professionals on staff, independent contractors, suppliers, agents, and clinic-based physicians, etc. This policy enables the HIPAA Privacy Compliance Officer to review contracts and obligations (seeking the advice of legal counsel, where appropriate) that may contain issues that could violate HIPAA Privacy provisions and other legal or regulatory requirements.

Notice of Privacy Practices

Even though business associates are not required to use a Notice of Privacy Practices, it is important for you to know what their function is.

The Notice of Privacy Practices (NPP**)** is a **statement** from the provider to the patient on how the patient's **PHI will be handled and protected** by the provider's office. The NPP must be provided on or before the first delivery of service, except in emergency situations. Direct care providers are obligated to make a good faith attempt to obtain an individual's written acknowledgement that they have received a copy of the NPP. Even if the individual fails to return the acknowledgement to the provider, the provider will be deemed to have made the required "good faith" attempt to obtain the written acknowledgement. There are certain required elements that the NPP must contain. The patient must receive a complete version of the NPP. The provider must display the entire notice in a prominent place in the provider's office.

Treatment does not depend on the signed receipt of the Notice. The Notice is only a statement of how you are handling the patient's PHI. The patient does not have the right to approve or disapprove of the content of the NPP.

Business Associates and Subcontractors

Business Associates of covered entities and their subcontractors **must comply directly and independently** with the HIPAA Security and Privacy Rules, according to the Health Information Technology for Economic and Clinical Health (HITECH) Act. The Security Rule, which complements the HIPAA Privacy Rule, includes safeguards for protecting patients' electronic protected health information (PHI), based on three components:

- **Administrative**: Organizations must have procedures that show how they will comply with the security rule
- **Physical**: Organizations must control how patients' records are physically accessed and prevent inappropriate access
- **Technical**: Organizations must have a system to control computer access and monitor and protect communication that flows electronically over open networks.

Section 13401 of the HITECH Act includes the **new BA requirements**. The act also states that civil and criminal penalties for violations of the HIPAA and compliance audits apply directly to BAs. Covered entities must incorporate these additional requirements in their agreements with BAs, according to the new law.

A covered entity may disclose PHI to a business associate for purposes agreed to by contract.

HHS' definition of a Business Associate:

- A business associate is a person or entity who provides certain functions, activities, or services **on behalf of** a covered entity involving the use and/or disclosure of PHI.
- A business associate is **not** a member of the health care provider's workforce.
- A health care provider or other covered entity can also be a business associate to another covered entity.
- Covered entities who disclose PHI to providers for treatment are **not business associates**.

An insurance company is **not** a business associate. They do not perform a function on behalf of a covered entity.

The provider's office must document by means of a written contract or other written agreement the satisfactory assurances that the business associate will appropriately safeguard the information disclosed to them for their use.

Examples of a business associate are:

- A billing company
- A clearinghouse
- An answering service
- A document shredding company
- A collection agency
- An attorney
- Couriers

The contract with business associates covers a set of contractual obligations. Their function is to protect information generally and help the covered entity comply with the entity's obligations under HIPAA.

HHS has stressed that PHI may be disclosed to a business associate **only** to help the providers and plans carry out their health care functions - **not for independent use** by the business associate**.**

Organized Health Care Arrangement (OHCA)

This is an agreement between multiple covered entities involved in an integrated care setting that allows each member to act on behalf of the whole. If a covered entity is part of an OHCA, the services rendered to patients while under the auspices of the OHCA are covered under a group NPP. For example, if a

health care provider sees patients at a hospital with which (s) he is part of an OHCA, the hospital's NPP is sufficient and the provider does not need one for the hospital services. However, another NPP will be needed for services rendered at the provider's office.

Modifications

HHS has said that they can and will issue proposed modifications to correct any unintended negative effects of the Privacy and Security Rules on health care quality or on access to such care. The modifications will be posted in the Federal Register for a period of time for comments before any new provision goes into effect.

Retention of HIPAA-related records

The HIPAA regulations require that all HIPAA related records and documents be retained for 6 years. This applies to authorizations, audit records, business associate agreements and contracts, etc. They may then be destroyed in a manner that does not allow for disclosure of any PHI (burning, shredding, etc.).

This **does not** apply to retention of medical records. That record retention period is determined by your state laws.

Acronyms

BA - Business Associate

CE - Covered Entity

CMS - Center for Medicare/Medicaid Services

DRS - Designated Record Set

EDI - Electronic Data Interchange

EPHI - Electronic Protected Health Information

HIPAA - Health Insurance Portability and Accountability Act

HHS - Health and Human Services

LDS - Limited Data Set

NPP - Notice of Privacy Practices

NEI - National Employer Identifier

NPI - National Provider Identifier

OCR - Office for Civil Rights

OHCA - Organized Health care Arrangement

OHS - Office of HIPAA Standards

PHI - Protected Health Information

TPO - Treatment Payment Health care Operations

TCS - Transactions and Code Sets

Treatment, Payment, or Healthcare Operations (TPO)

Under the HIPAA Privacy Rule, covered entities and business associates are **permitted** to disclose PHI **without a signed authorization** for treatment, payment, or health care operations reasons. Examples:

- Doctors and/or Hospitals (that are covered entities) may share information freely with one another for treatment reasons.
- Patients' information may also be released without their authorization to insurance companies in order to receive payment for services provided.
- Health care operations can include a variety of business activities including but not limited to quality assessment, employee review, licensing, etc.

Any uses or disclosures of PHI for **non-TPO are not permitted** unless they are required by state or other law, or have been authorized by the patient. Descriptions of treatment, payment, and health care operations are on the NPP.

Healthcare Operations

The HIPAA Privacy Rule's definition of "health care operations" include those activities that enable you to conduct a viable business and to perform those "covered functions" that make you a business associate or health care provider. Some examples of health care operations include:

- Scheduling appointments, surgeries, and pre-admission activities
- Population-based analyses or records reviewed for treatment protocol development or modification
- Supervised health care training
- Activities related to the improvement of payment and coverage methods

Payment

Payment is a defined term that encompasses the various activities of business associates and health care providers to obtain payment or be reimbursed for their services. In addition to the general definition, the Privacy Rule provides examples of common payment activities that include, but are not limited to:

- Determining eligibility or coverage under a plan and adjudicating claims;
- Risk adjustments;
- Billing and collection activities;
- Reviewing health care services for medical necessity, coverage, justification of charges, etc.;
- Utilization review activities; and
- Disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his or her payment history, and identifying information about the covered entity).

Required Uses and Disclosures of PHI

HIPAA Privacy **requires** only two types of disclosures of PHI:

- To the patient about whom the PHI applies
- To HHS to investigate or determine compliance with HIPAA

These are the only two uses and disclosures that are **required**. The patient's authorization is not required.

Authorization

The Privacy Rule **requires patient authorization** for **non-TPO** uses and disclosures of PHI.

An authorization is a customized document that gives covered entities permission to use **specified PHI for specified purposes**, which are generally other than TPO, or to disclose PHI to a third party **specified** by the individual. Business associates and covered entities may not condition treatment or coverage on the individual providing an authorization. An authorization is detailed. It covers only the uses and disclosures and only the PHI stipulated in the authorization, it has an expiration date, and it also states the purpose for which information may be used or disclosed.

An authorization is required for use and disclosure of PHI not otherwise allowed by the Privacy Rule. All business associates and covered entities, not just direct treatment providers, must obtain an authorization to use or disclose PHI for these purposes. For example, a covered entity would need an authorization from individuals to sell a patient mailing list, to disclose information to an employer for employment decisions, or to disclose for eligibility for life insurance.

The Privacy Rule requires business associates and providers to obtain an authorization to use or disclose PHI maintained in psychotherapy notes for treatment by persons other than the originator of the notes, for payment, or for health care operations purposes.

The authorization for HIPAA Privacy uses and disclosures should not be confused with the **consent to treat** form. The consent to treat form gives the health care provider permission to treat the patient and is **governed by state law**. It is not governed at all by HIPAA.

Restriction for Use and Disclosure of PHI

Patients have the right under the HIPAA Privacy Rule to request a restriction on certain types of uses and disclosures of their protected health information. Business associates and health care providers must permit this request but do not have to agree with the requested restriction. Here is how that part of the Privacy Rule works with a list of the types of uses and disclosures:

A business associate or health care provider must permit an individual to request that they restrict:

- Uses and disclosures of PHI about the individual to carry out payment or health care operations; and
- Uses and disclosures for involvement in the individual's care and notification purposes when the patient is present, such as -
- Disclosures of (with the patient's agreement) PHI to a family member or other person involved with the patient's care
- Limited uses and disclosures of PHI when the individual is not present if –
- The provider uses professional judgment and experience with common practice to make reasonable inferences to the individual's best interest.
- Uses and disclosures of PHI for disaster relief purposes.

A health care provider is not required to agree to a restriction except if the restriction is to a health plan regarding a service for which the patient has paid in full.

If a restriction agreement is made, it can also be terminated. A business associate or health care provider may terminate his or her agreement to a restriction if:

- The individual agrees to or requests the termination in writing
- The individual orally agrees to the termination and the oral agreement is documented; or
- The business associate or provider informs the individual that he or she is terminating the agreement to a restriction, except that such termination is only effective with respect to PHI created or received after he or she has so informed the individual

When this restriction agreement is terminated, it must be documented and maintained in written or electronic form.

Exception: The patient has the right to request a restriction on the use and disclosure of PHI if the services about which the PHI refers is paid in full by the patient and the disclosure is for payment purposes to a health plan. If those conditions are met, then the provider or business associate is required to honor the request for the restriction.

Uses and Disclosures without Authorization

Although the general rule is that uses disclosures can be made only with the patient's authorization, there are a few cases where the patient's authorization is not necessary. A few of the most common **allowable** are:

- Any disclosure made for TPO reasons
- Domestic violence, abuse, or neglect, as well as cases of child abuse or neglect
- A court order or subpoena
- A use or disclosure for public health reasons to the proper authorities
- A use or disclosure required by law to law enforcement for a criminal investigation
- A use or disclosure required by law to report cases of suspicious deaths or suspected crime victims

Disclosure of an Entire Medical Record

HHS has stated that the Privacy Rule does not prohibit use, disclosure, or requests of an entire medical record. HSS has also said that a business associate or covered entity may use, disclose, or request an entire medical record without a case-by-case justification **if** the business associate or covered entity has **documented in its policies and procedures** that the entire medical record is the amount reasonably necessary for certain identified purposes.

Minimum Necessary Standard

HHS requires that each business associate and health care entity determine its own set of standards for minimum necessary use and disclosure of PHI. This means a business associate or covered entity must make **reasonable** efforts to limit use, disclosure of, and requests for PHI to the **minimum necessary to accomplish the intended purpose**.

To allow business associates and covered entities the flexibility to address their unique circumstances, the rule requires them to make their own assessment of what PHI is reasonably necessary for a particular purpose, given the characteristics of their business and workforce.

The minimum necessary provisions **do not** apply to the following:

- Disclosures to or requests by a health care provider for **treatment purposes**.
- Disclosures to the **individual** who is the subject of the information.
- Uses or disclosures made pursuant to an **authorization** requested by the individual.
- Uses or disclosures required for **compliance** with the standardized Health Insurance Portability and Accountability Act (HIPAA).
- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the rule for **enforcement** purposes.
- Uses or disclosures that are **required by law**.
- Prior to April 14, 2003

It is very important to remember that with respect to a business associate's or covered entity's use of PHI, the Privacy Rule requires that they identify:

- Those persons or classes of persons, as appropriate, in its workforce who need access to PHI to carry out their duties; and
- For each such person or classes of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.

Each business associate and covered entity must make reasonable efforts to limit the access of each person or classes of persons to the PHI for which access is needed.

Reasonable Reliance

Even though minimum necessary does not apply to treatment, there is also a reasonable reliance policy to consider. If a request for patient information is seeking more than the minimum necessary PHI, the Privacy Rule requires you to limit the disclosure to the minimum you think is necessary using a reasonable effort to limit patient information while providing the best care for the patient.

However, if another treatment provider requests the disclosure of PHI to them, you may reasonably rely that their request is for the minimum necessary for their purpose. This also applies to requests from a public official, a professional (such as an attorney or accountant who is a covered entity's business associate), or a researcher who provides documentation required by the Privacy Rule (See "Research"). In turn, when your office is requesting PHI from another provider, you must determine what the minimum necessary is for your purpose when your request is made.

Incidental Uses and Disclosures

These disclosures are non-intentional and occur as a by-product of allowed uses and disclosures. They are allowed as long as the minimum necessary standard and reasonable safeguards are applied in the course of your everyday operations. An example would be if a passerby overhears PHI being discussed at a nursing station. These disclosures do not have to be accounted for.

Accounting for Uses and Disclosures

Under HIPAA Privacy, the patient has many rights. One of these is the right to request an accounting of all **non-TPO** disclosures (any disclosure that is not for treatment, payment, or health care operations). For this reason, it is required that you maintain a disclosure log. **Anytime** information is disclosed for a non-TPO purpose, except for "incidental disclosures", it must be documented on the "Log for PHI Disclosures" form. For example, if a disclosure is made to an attorney, to a school, or to a public health agency, the disclosure should be added to the Log for PHI Disclosures form. That way, if the patient were to request the accounting of non-TPO disclosures (use the Request for Accounting of PHI Disclosures form), the log is already up-to-date. Simply provide the patient with the information contained on the log. The patient may receive an accounting free once in a 12-month period.

Even though most **non-TPO** uses and disclosures of PHI have to be logged, there are a few exceptions. Examples of disclosures that **do not** have to be accounted for are:

- For disclosures pursuant to an authorization
- For reporting abuse and neglect
- For National Security and/or Intelligence purposes
- To a Correctional Institution or Law Enforcement Officer having lawful custody of an inmate about whom the PHI applies

- The PHI is part of a Limited Data Set
- The disclosure occurred prior to 4/14/03

Accidental Disclosures

These types of disclosures are distinctly different from incidental disclosures. Accidental disclosures happen when a mistake is made in disclosing a patient's PHI. Examples include faxing or mailing PHI to the wrong destination or disclosing PHI to an unauthorized person. If you are aware of an accidental disclosure, you need to log the disclosure on the disclosure log. If the disclosure is potentially harmful or damaging to the patient, you need to notify the patient of the accidental disclosure.

Mitigation

If a covered entity **accidentally** discloses PHI for a reason that is not allowed or required under the Privacy Rule or any other law the entity must take action necessary to repair the harm done by the disclosure. If the disclosure is apt to cause harm to the patient, the covered entity must inform the patient of the disclosure. This type of disclosure is **not considered an incidental disclosure** and needs to be accounted for in the patient's "PHI Disclosure Log." You must also change your policies and procedures to ensure the same situation does not reoccur.

Example: The office receives a request from a health care provider to fax over protected health information of a patient for treatment reasons. In preparing the information one of your staff mixes up the fax number with another office's fax number and as a result your office accidentally faxes the PHI to the wrong doctor's office.

In order to successfully mitigate this situation you would need to contact the office you sent the information to and ask them to destroy it. You would need to document the accidental disclosure as well as document the checks (what you did to find out the problem) and corrective action (what you did to fix the problem). You must also document, depending on the seriousness of the disclosure, whether or not you contacted the patient and why. This type of effort would leave the harm successfully mitigated.

Photographs

In your office or practice you may need to keep photographs of patients. The usage of photographs is within HIPAA Privacy guidelines as long as these photographs are kept away from public view. If you, however, use a patient's photographs in a place where they can be seen by the public for use as demonstration of your organization's skills and techniques, the patient's authorization must be obtained.

Faxes and E-mails

Under HIPAA, faxes and e-mails that contain PHI are allowed for TPO purposes. All faxes and e-mails sent from your office need to have the disclaimer attached. Be sure the fax machine is located in an area that is secure and removed from unauthorized access.

You need to ensure that the faxes sent from your office for TPO purposes are sent to the correct destination. You must verify the fax number to which you are faxing. It is recommended that you log your faxes as a good way to track them.

Note: If your FAX and E-mail communications do not display an adequate privacy warning, add the following to them promptly and permanently:

PRIVILEGED AND CONFIDENTIAL: This document and the information contained herein are confidential and protected from disclosure pursuant to Federal law. This message is intended only for the use of the Addressee(s) and may contain information that is PRIVILEGED and CONFIDENTIAL. If you are not the intended recipient, you are hereby notified that the use, dissemination, or copying of this information is strictly prohibited. If you have received this communication in error, please erase all copies of the message and its attachments and notify the sender immediately.

Marketing

Marketing refers to the communication about a product or service that encourages recipients of the communication to purchase or use the product or service unless it is for treatment purposes.

You need a written authorization allowing you to disclose the patient's PHI if you have **any intent** to sell, transfer, or use the PHI for commercial advantage or personal gain. This carries maximum penalties under federal law, $500,000, 10 years imprisonment, or both.

If you hire a person or company to conduct marketing activities on **your behalf**, you must enter into a business associate contract with them.

It is **not marketing** for a business associate or covered entity to use an individual's PHI to tailor a health-related communication to that individual, when the communication is:

- Part of a provider's treatment of the patient and for the purpose of furthering that treatment.
- Made in the course of managing the individual's treatment or recommending alternative treatment.

HHS has indicated that if a communication is marketing, you may make the communication **without an authorization** only in the following circumstances:

- It is a face-to-face communication with the individual.
- It involves products or services of nominal value

For **all** other communications that are "marketing" under the Privacy Rule, you must obtain the individual's authorization to use or disclose PHI to create or make the marketing communication.

(See the "Standard Authorization" form)

Research

Research is the systematic investigation, development, testing, and evaluation designed to develop **generalized knowledge**. HHS has made the Privacy Rule to protect PHI, while at the same time, ensuring that researchers continue to have access to medical information necessary to conduct vital research.

De-identified health information

A business associate or covered entity may use or disclose for research purposes health information which has been de-identified. De-identified health information has had identifiers removed. It is health information that does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. De-identified information has had most of the same identifiers removed as in a Limited Data Set. (See Limited Data Set)

Research Use/Disclosure with Individual Authorization

The Privacy Rule also permits business associates and covered entities to use and disclose PHI for research purposes when a research participant **authorizes** the use or disclosure of information about him or herself. To use or disclose PHI created from a research study that includes treatment (e.g., a clinical trial), additional research-specific elements must be included in the authorization form which describe how PHI created for the research study will be used or disclosed. The authorization must describe types of information that will be provided to the health plan. This authorization may be combined with the traditional informed consent document used in research.

Limited Data Sets

The Privacy Rule permits the use and disclosure of "limited data sets" of PHI for the purpose of **research**, public health, or health care operations. These limited data sets may be used in lieu of obtaining an authorization. These limited data sets do not include direct identifiers and may only be used or disclosed subject to the terms of a data use agreement. Limited data sets include the following:

1. Names
2. Address
3. Telephone numbers
4. Fax numbers
5. Electronic mail address
6. Social Security number
7. Medical Record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. Certificate/license numbers
11. Vehicle identifiers and serial numbers
12. Web Universal Resource Locators (URLs)
13. Internet Protocol (IP) address numbers
14. Bio-metric identifiers, including finger and voice prints
15. Full face photographic images and any comparable images

Data Use Agreement

In order to use limited data sets, a data use agreement must be used. The data use agreement must establish the permitted uses and disclosures of the data set consistent with the purpose of the disclosure. The agreement must also require the recipient of the limited data set to:

- Use the PHI contained in the set only as permitted under the Privacy Rule
- Limit who can use or receive the data
- Agree not to re-identify the data or contact the individual subjects of such data

- Use appropriate safeguards to prevent use or disclosure of the limited data set other than as permitted by the data use agreement and the Privacy Rule, or as required by law.

Research Use/Disclosure Without Individual Authorization

HHS has said that to use or disclose PHI **without authorization** by the research participant, a business associate or covered entity must obtain one of the following:

- Documentation that an alteration or waiver of research participants' authorization for use/disclosure of information about them for research purposes has been approved by an Institutional Review Board (IRB) or a Privacy Board.

or

- Representations from the researcher, either in writing or orally, that the use or disclosure of the PHI is solely to prepare a research protocol or for purposes preparatory to research; the researcher will not physically remove any PHI from the business associate or covered entity, **and** representation that PHI for which access is sought is necessary for the research purpose.

or

- Representations from the researcher, either in writing or orally, that the use or disclosure being sought is solely for research on the PHI of decedents; that the PHI being sought is necessary for the research**,** *and,* at the request of the business associate or covered entity, documentation of the death of the individuals about whom information is being sought.

A business associate or covered entity may use or disclose PHI for research purposes pursuant to a waiver of authorization by an IRB or Privacy Board provided it has obtained documentation of **all** of the following:

- A statement that the alteration or waiver of authorization was approved by an IRB or Privacy Board that was composed as stipulated by the Privacy Rule;
- A statement identifying the IRB or Privacy Board and the date on which the alteration or waiver of authorization was approved;
- A statement that the IRB or Privacy Board has determined that the alteration or waiver of authorization, in whole or in part, satisfies the following criteria:
- The use or disclosure of PHI involves no more than minimal risk to the individuals, based on, at least, the presence of the following elements:
- There is an adequate plan to protect the identifiers from improper use and disclosure;
- An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law, and;

- Adequate written assurances that the PHI will not be used or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI would be permitted
- The research could not practicably be conducted without the waiver or alteration; and
- The research could not practicably be conducted without access to and use of the PHI

The privacy board must review the proposed research and may use an expedited review procedure. The documentation of the alteration or waiver of authorization must be signed by the chair (or other member designated by the chair) of the IRB or Privacy Board.

If you are going to raise funds for the benefit of your organization, you may use (or disclose to a business associate) the following PHI without the patient's authorization:

- Demographic information relating to an individual

And

- Dates of health care provided to an individual

If you send fundraising materials to a patient, you must include information on how they can "opt-out" of the fundraising activities. If a patient chooses to "opt-out "or not participate in your fundraising activities, you must be certain not to include that patient in future fundraising communications or mailings.

Consumer Credit Reporting Agencies

The Privacy Rule allows disclosures to consumer reporting agencies. These disclosures, however, are limited to the following PHI about the individual:

- name
- address,
- date of birth,
- social security number,
- payment history, and
- account number.

In addition, disclosure of the name and address of the business associate, health care provider or health plan making the report is allowed.

Debt Collection Agencies

The Privacy Rule permits the use of services of debt collection agencies. Debt collection is recognized as a payment activity within the "payment" definition. HHS has stated that obtaining information about the location of the individual is a routine activity to facilitate the collection of amounts owed and the management of accounts receivable.

Compliance with any limitations placed on location information services by the Fair Debt Collection Practices Act would still apply.

Public Health

The Privacy rule allows the sharing of information that specifically may affect the public health with the proper authorities. The Privacy Rule allows disclosures that are required by law. Furthermore, disclosures to public health authorities that are authorized by law to collect or receive information for public health purposes are also permissible under the Privacy Rule. The Privacy Rule continues to allow for the existing practice of sharing PHI with public health authorities that are authorized by law to collect or receive such information to aid them in their mission of protecting the health of the public.

Psychotherapy Notes

Psychotherapy notes are notes that are recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversations during a private counseling session or a group, joint, or family counseling session and that are **separated** from the rest of the individual's medical record. Psychotherapy notes **exclude** medication prescription and monitoring, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Authorization Required

A business associate or healthcare provider must **obtain an authorization** for any use or disclosure of psychotherapy notes **except**:

- To carry out the following treatment, payment, or healthcare operation

    1. Use by the **originator** of the psychotherapy notes for treatment

2. Use or disclosure by the business associate or healthcare provider for its own **training program** in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, or individual counseling; or

3. Use or disclosure by the business associate or healthcare provider to defend itself in a **legal action** or other proceeding brought by the individual

- A use or disclosure that is required by the Secretary of the Department of Health and Human Services to investigate or determine the business associate's or healthcare provider's compliance.
- A permitted use or disclosure that is required by law.
- A permitted use or disclosure with respect to the oversight of the originator of the psychotherapy note
- A permitted use or disclosure to a coroner or medical examiner for the purpose of identifying a deceased person.
- A permitted use or disclosure that is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

Sign-In Sheets

Sign–in sheets are permitted by the Privacy Rule as long as the only information listed on them is the minimum necessary information. That would include:

- the patient's name,
- appointment time,
- doctor's name
- the patient's time of arrival for the appointment.

Other identifying information would be prohibited.

Call Verification

HIPAA Privacy requires you to verify the identity of an individual calling to seek his or her own PHI over the telephone. You may assign a password or other particular piece of information in advance that the patient must use to identify himself. Examples include:

- a password,
- the patient's social security number (either the whole number or part of the number)",

- date of the patient's birth,
- zip code,
- mother's maiden name, or
- a combination of codes.

Social Security Numbers

Because of the great pressure to keep health information any other personal information protected, many states have passed laws that restrict practices, insurance companies, or other types of businesses from requiring an individual to disclose their entire social security number. Some practices use the last four digits of a patient's social security number to verify the identity of the person they are talking to. This type of verification is still allowed because you are not requesting their entire number. This is still a great way to verify patients, but be careful about requiring a full disclosure of a social security number because **many states now make such a requirement unlawful**.

Phone Messages and Appointment Reminders

Reminder cards or postcards can still be sent out to your patients, but the information on the card must be limited to the **minimum necessary** and contain **no PHI**. You may list on the card:

- the patient's name,
- the date and time of the appointment but
- **not** the reason for the appointment.

Use a sealed envelope to send a patient any other additional information that could be considered PHI.

If you want the patient to call to **schedule an appointment**, you must **not mention the reason** for the appointment. You may also leave messages for your patients on an answering machine or with a third party. The only information you may leave, if calling the patient about **test results**, is:

- the name and phone number of their doctor and
- that you would like the patient to return your call.

If you are calling the patient to **remind them of an appointment**, you may leave:

- the name of the patient,
- the name of their doctor, and
- the date and time of the appointment.

You may **not** include in your message the reason for the appointment.

Reasonable Safeguards

These are administrative, physical and technical measures that are tailored to your practice and designed to reasonably protect physical and electronic protected health information.

HHS has said that health care providers may need to make certain adjustments to their facilities to minimize access, such as isolating and/or locking file cabinets or records rooms, or providing additional security, such as passwords, on computers maintaining personal information. Fax machines and telephone answering systems should be place in a secured area. These safeguards are to be determined by the particular provider depending on the circumstances and working conditions of the particular office. The provider must take reasonable precautions to prevent inadvertent or unnecessary disclosures of PHI.

The Privacy Rule **does not require** the following types of structural or systems changes:

- Private rooms.
- Soundproofing of rooms.
- Encryption of wireless or other emergency medical radio communications which can be intercepted by scanners.
- Encryption of telephone systems.

Some examples given by HHS of the types of adjustments or modifications to facilities or systems that may constitute reasonable safeguards are:

- Pharmacies could ask waiting customers to stand a few feet back from a counter used for patient counseling.
- Providers could add curtains or screens to areas where oral communications often occur between physicians and patients or among professionals treating the patient.
- Use of cubicles, dividers, shields, or similar barriers may constitute a reasonable safeguard.
- Speaking quietly may be appropriate.
- The front of our patient files should be marked "confidential" with either a label or a stamp. All correspondence that the office receives by either mail or fax that contains PHI, should also be marked "confidential".
- When in use, patient charts could be turned away from public view.
- Fax machines and telephone answering systems could be placed in a secured location.

HHS does not expect reasonable safeguards to guarantee the privacy of PHI from any and all potential risks.

Oral Communication

HHS has stated that the Privacy Rule applies to all forms of PHI including PHI in oral form.

The Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. The rule only requires covered entities to implement **reasonable safeguards** that reflect their particular circumstances to **ensure that providers' primary consideration is the appropriate treatment of their patients.**

HHS has also said that they also understand that overheard communications are unavoidable. For example, in a busy emergency room, it may be necessary for providers to speak loudly in order to ensure appropriate treatment. HHS will consider the following practices to be permissible if reasonable precautions are taken to minimize the chance of inadvertent disclosures to others:

- Health care staff may orally coordinate services at hospital nursing stations.
- Nurses or other health care professionals may discuss a patient's condition over the phone with the patient, a provider, or a family member involved with the patient's medical care.
- A health care professional may discuss lab test results with a patient or other provider in a joint treatment area.
- Health care professionals may discuss a patient's condition during training rounds in an academic or training institution.

Calling out the patient's name in the waiting room is not disclosing PHI. The **name** only can be mentioned but not any other direct identifiers such as street address, telephone number, social security number, reason for visit, etc.

Visitors

The HIPAA Privacy Rules specifically addresses the need to prevent unauthorized individuals from access to areas in your office that are a source of patient information whether verbal, written, or electronic. These visitors might include but are not limited to:

- drug company representatives,
- office machine repair personnel,
- janitorial service workers, etc.

If you are applying the minimum necessary standard and reasonable safeguards, any disclosures of PHI to these visitors would be considered incidental disclosures. They are **not** considered business associates.

Also, these visitors would not include family members who accompany the patient and are involved in the patient's medical care.

Handling E.O.B.s

During the course of billing a secondary insurance carrier, you will send a copy of the primary insurance EOB (explanation of benefits). There may be other patients' PHI also on the EOB. Be sure to black out or white out the PHI that does not apply to the claim. Covered entities are responsible for all uses and disclosures of PHI. Every use and disclosure must be conducted for an allowed reason or have a legitimate reason associated with it. If not, it is considered to be a violation of the HIPAA Privacy law.

Auditing

The provider should randomly select a group of patient records. This procedure should be done every six months. The audit forms provided are to be used to perform billing, privacy and safeguard audits, not only to check for HIPAA violations but also to prevent billing mistakes that would result in the practice having fines or decreased revenue from billing errors.

Simple mistakes could possibly put your office under investigation from HHS or a payer. This could lead your office to being placed on the HHS or payer's focus list leading to possibly:

- Delayed Payment
- Criminal Investigation
- Audit
- Compliance Review

Patient's Right of Access

HIPAA provides all individuals with the right to access their PHI maintained in a designated record set by their health care providers who create or receive their PHI. The right must be provided for as long as PHI is maintained in a designated record set.

A **"designated record set"** is one containing information utilized and maintained for the purpose of making decisions about an individual's health care. Patients have the right to access PHI used to make decisions about them, including, for example, information upon which health care decisions are based and information to determine payment. Information maintained, but not used to make decisions about the patient, falls outside the designated record set and is exempt from access.

When a patient requests in writing the opportunity to inspect or copy their PHI, this **checklist** ensures that your practice is following **HIPAA rules and regulations:**

- The request must be in writing
- You must act upon the request within 30 days if PHI is accessible on-site
- You must act upon the request within 60 days if PHI is accessible off-site
- You must act upon the request within 90 days if PHI is accessible off-site and you have given written notice to the patient of that time frame in writing within the first 30 days of the request

Form of the access requested:

- You may provide access to PHI in summary form if the individual has previously agreed to receive it in that manner
- You may charge a reasonable fee for copying the records requested but not for the retrieval of the records

Denial of Access

You may deny the individual access to their PHI if you have **reviewable** grounds for denial. You are **not required and/or allowed by law to allow access to:**

- Psychotherapy notes
- Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding
- If you are acting under the direction of a correctional institution
- If the PHI is contained in records that are subject to the Federal Privacy Act of 1964 (not HIPAA Privacy)
- If the PHI was obtained from someone other than a health care provider under a promise of confidentiality
- If the access requested is reasonably likely to cause substantial harm to another person

If denial of access is decided upon for any reason, the provider must provide a timely written denial ("Denial of Request to Inspect or Copy PHI") to the authorized individual requesting the PHI. The provider must also allow access to the information that was not denied. After issuing a denial, if the

authorized individual does not agree with the denial determination they have the right to request a review of the denial. They also have the right to submit a complaint to the practice or to the Secretary of Health and Human Services.

If the authorized individual requests a review of the denial the covered entity must designate someone in the office that was not a part of the first decision, to review the denial in a reasonable period of time and submit a final decision to the patient.

Denials always fall into two categories, "reviewable" and "unreviewable". This is very important to understand when making a decision able a review of denial request. If the reason for the denial falls on unreviewable grounds, then the practice is not allowed to disclose such information. On the other hand if the denial falls on reviewable grounds, then you are allow to continue with the review process.

The following are **reviewable grounds** for denial:

- A licensed health care professional has determined, in the exercise of professional judgment, that the access requested by the patient or an authorized individual makes reference to another person (unless such other person is a health care provider) and
- The disclosure is reasonably likely to endanger the life or physical safety of the individual or another person, or
- For any other reason the PHI is reasonably likely to endanger the life or physical safety of the individual or another.

The following are **unreviewable grounds** for denial:

- There is no right of access under HIPAA (psychotherapy notes, PHI acquired under a promise of confidentiality, PHI compiled in anticipation of a civil, criminal or administrative action, abuse or neglect);
- A covered entity that is a **correctional institution** or a covered entity acting under the direction of the correctional institution may **deny**, in whole or in part, an inmate's request to obtain a copy of PHI, if obtaining such copy would jeopardize the **health, safety, security, custody**, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate;
- An individual's access to PHI created or obtained by a covered entity in the course of **research** that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when first consenting to participate in the research and the covered entity has informed them that the access will be reinstated upon completion of the research; or
- An individual's access to PHI that is contained in records that are subject to the **Privacy Act, 5 U.S.C. 552a**, may be denied, if prohibited by that law.

If the health care facility does not have the records the authorized individual is requesting they must refer them to the appropriate contact that maintains possession of their records.

Another consideration at this time would be to consult your state laws on the matter of patient access rights. Some state laws grant the patient more rights of access than HIPAA Privacy. States also determine the period of time for which the records need to be kept available.

HIPAA requires a 6-year period of record retention for HIPAA related documents but that may or may not apply to medical records depending upon your state law.

Destruction of Medical Records

If either paper or electronic files (including hard or soft disks) are to be disposed of, make certain they are erased, shredded or disposed of properly so they do not have the potential of being disclosed wrongfully. You will be responsible for any wrongful disclosures for failure to properly destroy PHI.

Patient Access to the Entire "Designated Record Set"

Before the implementation of HIPAA, health care providers in many states were able to give patients access only to the records created by their own office. They were not able to grant access to those records of the patient that were obtained from another practitioner. Patients had to go to each office that had originated each part of their medical record even if their current doctor had the entire record they needed. Now under HIPAA, covered entities are able to grant access for the patient to inspect or copy all of their protected health information in their **designated record set (DRS).**

HHS has stated that the patient and another treatment provider would be able to access the complete medical record including the portions that were created by other providers. This information has been used to make decisions about the patient in the past and may be vital to their continued treatment.

Fees for Copying

HIPAA allows you to charge a reasonable fee for your costs associated with the coping of medical records. You may not charge for the retrieval of those records, however. Fees for copying for most states have already been established. Most State laws specify the maximum of what practitioners can charge for copying medical records requested by a patient or the patient’s agent.

Amending Patient Records

Under HIPAA, patients have greater access to their personal records. Patients also have the right to amend parts of their record. They **do not** have the right to **change** any information within their record, but they can submit a written amendment to any part of their record. The covered entity is required to consider the request for an amendment but does not have to accept the amendment.

Patient's Right to Request Confidential Communication

Patients have the right to request that a provider's communications with them is made in a specified and confidential manner. For example:

- By telephone at work rather than at home
- In writing only
- By e-mail only

The request must be in writing, and the provider cannot refuse the request if the request is reasonable. The covered entity may not require an explanation from the individual as to the basis for the request as a condition of providing the confidential communication.

Personal Representative

A personal representative is to be treated as the patient with the same rights and authority. There are two classifications of a personal representative.

Deceased Individuals

A person who has been **legally designated** (legal guardian, executor of will, next of kin, power-of-attorney, etc.) to represent a patient is also referred to as a "**personal representative**" of the patient. This means that such a personal representative would be treated as if they were the individual, having all rights of access to the deceased person's protected health information. The key word is "legally" designated. Even if the person requesting the information is the "next of kin," it still must be legally documented and in accordance with your state law.

Parents and Minors

The Privacy Rule provides individuals with certain rights with respect to their PHI, including the right to obtain access to and to request amendment of health information about themselves. These rights rest with that individual, or with the "personal representative" of that individual. In general, a person's right to control PHI is based on that person's right (under state or other applicable law, e.g., tribal or military law) to control the health care itself.

The Privacy Rule generally allows parents to act as their child's **personal representative**. This allows them access to information about the health and well-being of their children when state or other underlying law allows these parents to make treatment decisions for their child. This would also be true in the case of a guardian or other person acting *in loco parentis* of a minor. But there are exceptions in which a parent might not be the **personal representative** with respect to certain health information about a minor child.

These exceptions apply to:

- When the **parent agrees** that the minor and the health care provider may have a **confidential relationship**, the provider is allowed to withhold information from the parent to the extent of that agreement.
- When the provider reasonably believes in his or her **professional judgment** that the child has been or may be subjected to **abuse or neglect.**
- When, in the provider's **professional judgment,** treating the parent as the child's personal representative could **endanger** the child.
- When **State** or other **law does not require consent** of a parent or other person before a minor can obtain a particular health care service and the minor consents to the health care service.
- When a court determines or other law authorizes someone other than the parent to make treatment decisions for the minor that authorized person would be the personal representative not the parent.

Immunization Records

In order to enroll a child in school, the school requires that parents provide proof of a child's immunization against communicable diseases. This immunization record contains the child's PHI.

Under HIPAA, if the parent furnishes the immunization record to the school themselves, no authorization is required. Under HIPAA, if the school requests the record from the health care provider's office, an authorization is no longer required before the record can be released to the school.

Emergency Medical Care

Providers are able to treat minor children in emergencies without the parent's consent, but generally the parent still remains the personal representative. Generally, they are still entitled to gain access to PHI regarding their child's care and treatment, unless in the use of professional judgement the physician suspect's abuse, neglect, or reasonably believes that releasing the information to the parent would endanger the child.

Disclosures to Law Enforcement

The Privacy Rule establishes new procedures and safeguards to restrict the circumstances under which you may give such information to law enforcement officers. For example, the rule limits the type of information that you may disclose to law enforcement, absent a warrant or other prior process, when law enforcement is seeking to identify or locate a suspect. It specifically prohibits disclosure of DNA information for this purpose, absent some other legal requirements such as a warrant. Similarly, under most circumstances, the Privacy Rule requires you to obtain permission from persons who have been the victim of domestic violence or abuse before disclosing information about them to law enforcement.

Some other federal or state law may require a disclosure, and the Privacy Rule does not interfere with the operation of these other laws. However, unless the disclosure is required by some other law, HHS has said that you should use your professional judgment to decide whether to disclose information, reflecting your own policies and ethical principles. In other words, HHS is allowing physicians, hospitals, and health plans to continue to follow their own policies to protect privacy in such instances.

Disclosures Allowed Without an Authorization

The Privacy Rule is balanced to protect an individual's privacy while allowing important law enforcement functions to continue. The Rule permits covered entities to disclose protected health information (PHI) to law enforcement officials, **without the individual's written authorization**, under specific circumstances summarized below:

Court-ordered Warrant or Subpoena

To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena. The Rule recognizes that the legal process in obtaining a court order and the secrecy of the grand jury process provides protections for the individual's private information.

Administrative Request or Subpoena

To respond to an administrative request, such as an administrative subpoena or investigative demand or other written request from a law enforcement official. Because an administrative request may be made without judicial involvement, the Rule requires all administrative requests to include or be accompanied by a written statement that the information requested is relevant and material, specific and limited in scope, and de-identified information cannot be used.

Applicable Law and Ethical Standard

To a law enforcement officially reasonably able to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; or to identify or apprehend an individual who appears to have escaped from lawful custody.

Averting a Serious Threat to Health and Safety

If you believe that your practice, a workforce member, a patient, or the public is in danger of a threat to health and safety, your disclosure of PHI for that purpose is protected under HIPAA. You may, consistent with law and ethical conduct, use or disclose PHI if you believe in good faith that:

- It is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public;

And

- It is reported to a person or persons reasonable able to prevent or lessen the threat, including the target of the threat

Or

It is necessary for law enforcement authorities to identify or apprehend an individual:

- Because of a statement by an individual admitting participation in a violent crime that you reasonably believe may have caused serious physical harm to the victim;

Or

- Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

Identifying an Individual

To respond to a request for PHI for purposes of identifying or locating a suspect, fugitive, material witness or missing person; but you must **limit** disclosures of PHI to name and address, date and place of birth, social security number, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death, and a description of distinguishing physical characteristics. Other information related to the individual's DNA, dental records, body fluid or tissue typing, samples, or analysis cannot be disclosed under this provision, but may be disclosed in response to a court order, warrant, or written administrative request.

This **same limited information** may be reported to law enforcement:

- About a **suspected perpetrator of a c**rime when the report is made by the victim who is a member of your workforce;
- To identify or apprehend an **individual who has admitted participation in a violent crime** that you reasonably believe may have caused serious physical harm to a victim, provided that the admission was not made in the course of or based on the individual's request for therapy, counseling, or treatment related to the propensity to commit this type of violent act

Victim of a Crime

To respond to a request for PHI about a victim of a crime, and the victim agrees. If, because of an emergency or the person's incapacity, the individual cannot agree, you may disclose the PHI if law enforcement officials represent that the PHI is not intended to be used against the victim, is needed to

determine whether another person broke the law, the investigation would be materially and adversely affected by waiting until the victim could agree, and you believe in your professional judgment that doing so is in the best interests of the individual whose information is requested.

Abuse, Neglect or Domestic Violence

All states have laws reporting the cases of suspected abuse and neglect. You should be familiar with your state law regarding these situations. They are very serious and need to be handled properly. In the case of child abuse, disclose information to a public health authority authorized to receive reports to prevent disease, injury, etc. or a government authority authorized to receive such reports. For victims of abuse, neglect, or domestic violence, report the situation to a government authority authorized by law to handle such cases. Proper procedure is to notify the victim of the disclosure. However, if you feel that doing so would put the individual at risk or cause serious harm to the individual or other victims, do not notify the individual. If the person(s) you suspect of committing the abuse or neglect is the patient's personal representative, you may elect not to treat that individual as the patient's personal representative.

Where child abuse victims or adult victims of abuse, neglect or domestic violence are concerned, these provisions of the Rule apply:

- Child abuse or neglect may be reported to any law enforcement official authorized by law to receive such reports and the agreement of the individual is not required.
- Adult abuse, neglect, or domestic violence may be reported to a law enforcement official authorized by law to receive such report

If the individual agrees;

If the report is required by law; or

If expressly authorized by law, and based on the exercise of professional judgment, the report is necessary to prevent serious harm to the individual or others, or in certain other emergency situations.

Notice to the individual of the report may be required.

Required by Law

To report PHI to law enforcement when required by law to do so. For example, state laws commonly require health care providers to report incidents of gunshot or stab wounds, or other violent injuries; and the Rule permits disclosures of PHI as necessary to comply with these laws.

Death of an Individual

To alert law enforcement to the death of the individual, when there is a suspicion that death resulted from criminal conduct.

- Information about a decedent may also be shared with medical examiners or coroners to assist them in identifying the decedent, determining the cause of death, or to carry out their other authorized duties.

Evidence of a Crime

To report PHI that the covered entity in good faith believes to be evidence of a crime that occurred on your premises.

Reporting a Crime on your Premises

If a crime was committed on the premises of your practice, you are protected under HIPAA to disclose that PHI that may help resolve the effects of the crime. You may disclose to a law enforcement official PHI that you believe in good faith constitutes **evidence** of criminal conduct that occurred on your premises.

Off-site Medical Emergency

When responding to an off-site medical emergency, as necessary to alert law enforcement about criminal activity, specifically, the commission and nature of the crime, the location of the crime or any victims, and the identity, description, and location of the perpetrator of the crime. This provision does not apply if the covered health care provider believes that the individual in need of the emergency medical care is the victim of abuse, neglect or domestic violence; see above Adult abuse, neglect, or domestic violence for when reports to law enforcement are allowed.

Governmental Law Enforcement

For certain other specialized governmental law enforcement purposes, such as:

- To federal officials authorized to conduct intelligence, counter-intelligence, and other national security activities under the National Security Act or to provide protective services to the President and others and conduct related investigations;
- To respond to a request for PHI by a correctional institution or a law enforcement official having lawful custody of an inmate or others if they represent such PHI is needed to provide health care to the individual; for the health and safety of the individual, other inmates, officers or employees of or others at a correctional institution or responsible for the transporting or transferring inmates; or for the administration and maintenance of the safety, security, and good order of the correctional facility, including law enforcement on the premises of the facility.

Except when required by law, the disclosures to law enforcement summarized above are subject to a **minimum necessary** determination by the covered entity. When reasonable to do so, the covered entity may rely upon the representations of the law enforcement official (as a public officer) as to what information is the minimum necessary for their lawful purpose. Moreover, if the law enforcement official making the request for information is not known to the covered entity, the covered entity must verify the identity and authority of such person prior to disclosing the information.

Subpoenas

You may disclose PHI for subpoenas or other civil processes only after obtaining "**satisfactory assurances**" that the person who is requesting the information has made a reasonable effort to provide written notice of the request to the individual whose records are the subject of the subpoena or that they have obtained a "**qualified protective order**". A "satisfactory assurance" is either a good faith effort to provide the patient with enough written notice to permit the patient to raise objections to disclosure, or an effort made to obtain a "qualified protective order" by having a written declaration and documentation of an order submitted to a court. A "qualified protective order" is an order of a court that prohibits the use of PHI for any purpose other than the case for which the records will be used. Keep in mind that only PHI expressly called for by the request may be disclosed or made available to the person requesting the patient's information. Check the subpoena for the following legally relevant information:

Check for the following:

- The identity of the person or court making the request.
- If the subpoena is issued in a federal court action, send only the precise information requested.
- If the subpoena is not issued in a court action, but by an administrative agency, determine if the agency is a "health oversight agency". If it is, then there is no need to determine whether the information requested is the minimum necessary.
- If the subpoena is issued by a state court, always check your local state laws for information about subpoena requests.

Satisfactory assurance is documentation that shows the requesting party's good faith attempt to provide written notice to the individual. The notice must include sufficient information about the litigation or proceeding to permit the individual to raise an objection to the court or administrative tribunal. Now if the request is accompanied by documentation of satisfactory assurance, you may release the information as long it contains the following: Documentation that the time to raise objections has passed and there were no objection filed, or all objection filed have been resolved and the disclosures being sought are consistent with the resolution. If the time has not passed or there are objections that have not been resolved you must not release the information.

A **qualified protective order** is an order from the court or administrative tribunal that prohibits parties from using PHI for any purpose other than the litigation it was requested for. It also requires that all parties must return to the covered entity or destroy all copies at the end of the litigation. The received request must be accompanied by documentation that sufficient effort has been made to secure a qualified protective order. Sufficient effort means that the parties of the dispute have agreed to a qualified protective order and have presented it to the court or administrative tribunal, or the party seeking PHI requested a qualified protective order from the court or administrative tribunal.

Disclosures by Whistleblowers

Workforce members who report employer violations are protected under HIPAA. A health care provider is not considered to have violated the HIPAA Privacy Rule if a member of its workforce or a business associate discloses PHI, provided that:

- The workforce member or business associate believes in good faith that the provider has engaged in conduct that is unlawful or otherwise violates professional or clinical standards or-
- The care, services, or conditions provided by the health care provider potentially endangers one or more patients, workers, or the public

and-

The disclosure is to:

- A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the health care provider or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the provider

or-

- An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the misconduct.

Disclosures by Workforce Member Crime Victims

If a workforce member becomes a victim of a crime, their reporting of that crime is protected under HIPAA. A health care provider is not considered to have violated the HIPAA Privacy Rule if a member of its workforce who is the victim of a criminal act discloses PHI to a law enforcement official, provided that:

- The PHI disclosed is about the suspected perpetrator of the criminal act, and the PHI disclosed is limited to:
- Name and address
- Date and place of birth
- Social Security number
- ABO blood type and rh factor
- Type of injury
- Date and time of treatment
- Date and time of death (if applicable)
- A description of distinguishing physical characteristics, including:
- Height
- Weight
- Gender

- Race
- Hair and eye color
- Presence or absence of facial hair
- Scars
- Tattoo’s

Health Oversight Activities

You are permitted to disclose PHI to a health oversight agency for oversight activities authorized by law including:

- Audits
- Civil, administrative or criminal investigations proceedings or actions
- Inspections
- Licensure
- Disciplinary actions
- Other appropriate oversight activities for:
  - The health care system
  - Government benefit programs
  - Government regulatory programs
  - Civil rights laws compliance

Health oversight activities **do not** include:

- Investigation of an individual
- The receipt of health care
- A claim for health care
- Qualification for health care

The Government's Role

In the Privacy rule, HHS has included governmental agencies among those who have to follow this new rule. Under the Privacy Rule, government-operated health plans and health care providers must meet

substantially the same requirements as private ones for protecting the privacy of PHI. In addition, government agencies must meet the requirements of the Privacy Act of 1974.

The HIPAA Privacy Rule does not require a physician or any other covered entity to send medical information to the government for a government database or similar operation. This rule does not require or allow any additional government access to medical information, with the one exception mentioned above: the rule does give the Office for Civil Rights (OCR) the authority to investigate complaints and to otherwise ensure that covered entities comply with the rule. While The Department of Health and Human Services issued the Privacy Rule, OCR has been assigned the responsibility of enforcing the Privacy Rule.

State Law Preemption

Not all state law is preempted by HIPAA. State laws that are more "stringent" than HIPAA, which basically means laws that require more protection of the privacy of information than HIPAA does, will still govern. For example, many states have laws applying a higher standard of confidentiality to particularly sensitive information, such as that relating to HIV/AIDS, psychotherapy notes, drug and alcohol information and genetic information. Comparing state laws requirements with the Privacy and Security Rules and requirements and current practices and policies of your office will identify gaps in current compliance requirements as well as future requirements necessitated by HIPAA.

Some state laws may be "contrary" to the HIPAA Privacy Rule. That means that the "contrary" state law would stand as an obstacle for HIPAA compliance. In that instance, HIPAA would be the prevailing law.

Social Security Numbers

Because of the great pressure to keep health information any other personal information protected, many states have passed laws that restrict practices, insurance companies, or other types of businesses from requiring an individual to disclose their entire social security number. Some practices use the last four digits of a patient's social security number to verify the identity of the person they are talking to. This type of verification is still allowed because you are not requesting their entire number. This is still a great way to verify patients, but be careful about requiring a full disclosure of a social security number because **many states now make such a requirement unlawful**.

Workers' Compensation

HIPAA does not generally apply to workers' compensation. The Privacy Rule permits covered entities to disclose PHI to workers' compensation insurers, State administrators, employers, self-insured

compensation plans and other persons involved in workers' compensation without the authorization of the individual. However, the disclosure must be required by law or needed for payment reason.

Training

HHS has said that ongoing training is required of covered entities in order to maintain ongoing compliance. There will be ongoing modifications in HIPAA that will require this regular, periodic training. This training must be documented by the covered entity.

Workforce Members

The employees or workforce members of your practice should have access to PHI on a "need-to-know" basis. That means the employees' degree of access to PHI would depend on the employees' job and what part of the patients' PHI they need access to in order to perform their jobs. The minimum necessary standard **does apply** to workforce members.

Medical Students and Other Medical Trainees

The minimum necessary requirements do not prohibit medical residents, medical students, nursing students, and other medical trainees from accessing patients' medical information in the course of their training. Medical residents, etc. must be trained on HIPAA rules and regulations as members of the workforce.

Employment Records

In your office, any employment records of your employees are **required** to be kept **completely** separate from any PHI (medical records). PHI must **never** by used by you as an employer for employment decisions.

However, when an employee authorizes disclosure of PHI you as his/her employer to substantiate sick leave, etc., those records then become part of the employment record and are no longer considered PHI.

Sanctions

The Privacy Rule states that "a covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity… (164.530(e) (1))." Sanctions are never fun to deal with, but they must be implemented to provide recourse for those that do not take HIPAA Privacy standards seriously. Take note that sanctions cannot be applied against whistleblowers or workforce member crime victims who are disclosing PHI to further their own case. You must not engage in intimidating or retaliatory acts against any individual who has filed a complaint, is testifying or assisting, participating in an investigation, compliance review, proceeding, or hearing. Also, you must not intimidate or retaliate against any individual who opposes acts or practices that are unlawful, provided the individual in good faith believes that the practice is unlawful and opposition is reasonable and does not disclose PHI in violation with HIPAA Privacy law.

Following are some examples of sanction policies to help you develop or improve your own policies. The violations have been divided into 3 levels of severity:

Level #1: Accidental Breach

Possible Scenarios– Employee does not log off the computer after use.

Employee faxes the wrong PHI to another practice.

Employee forgets to get a signed acknowledgment of receipt of the NPP.

Sanctions– Verbal warning documented in the employees file and mandatory re-education for the first offense. Continued offenses lead to progressive discipline up to and including termination.

Level #2: Intentional Breach without Harmful or Dishonest Intentions

Possible Scenarios– Viewing patient records out of curiosity.

Sharing PHI because the information is interesting (not for treatment purposes).

Employee shares computer password.

Sanctions – Written warning documented in the employee's file for the first offense. Could lead to discharge/dismissal with repeated offenses.

Level #3: Willful or Intentional Breach with Harmful or Dishonest Intentions

Possible Scenarios– Using PHI for personal gain (marketing without authorization).

Using PHI to cause harm.

Sanctions– Discharge/dismissal and possible legal action.

Please Note*: All applied sanctions must be documented.*

EDI Transactions

Congress and the health care industry have agreed that standards for the electronic exchange of administrative and financial health care transactions are **needed to improve the efficiency and effectiveness** of the health care system. The HIPAA law required the Secretary of Health and Human Services to adopt these standards.

EDI Transactions

As required by HIPAA, the Secretary of Health and Human Services has adopted standards for the following administrative and financial health care electronic transactions:

- Health claims and equivalent encounter information
- Enrollment and dis-enrollment in a health plan
- Eligibility for a health plan
- Health care payment and remittance advice
- Health plan premium payments
- Health claim status
- Referral certification and authorization
- Coordination of benefits

Standards for the first report of injury and claims attachments (also required by HIPAA) will be adopted at a later date.

You should obtain from your software vendor and clearinghouse documentation that they comply with the HIPAA TCS Standard. This can be accomplished by using the "HIPAA Transaction and Code Sets Compliance Assurance" form (in your "Forms" section) for both your software vendor and clearinghouse. You may still be in the process of complying with this standard, but ultimately you should obtain this documentation to ensure compliance in this area.

Code Sets

A code set is any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnosis codes, or medical procedure codes. Code sets for medical data are required

for data elements in the administrative and financial health care transaction standards adopted under HIPAA for diagnoses, procedures, and drugs.

The Secretary has adopted the following code sets as the standard medical data code sets*:*

- International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9-CM), Volumes 1 and 2
- International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9-CM), Volume 3 Procedures (**for inpatient claims only**)
- Current Procedural Terminology Fourth Edition (CPT-4) (CDT for dental procedures)
- Health Care Financing Administration Common Procedure Coding System (HCPCS)
- National Drug Codes (NDC) (**for retail pharmacy use only)**

Characterized as "smaller code sets" by HIPAA are sets of codes for data elements such as type of facility, type of units, and specified state within address fields. Familiar in this category are the U.S. Postal Service 2-character state abbreviations and zip codes. Other proprietary code sets will be eliminated if not explicitly mentioned in the Implementation Guides. The standards clarify that newly developed code sets may appear in response to the needs of future transaction standards.

Implementation Guides

Implementation Guides are necessary for a provider (usually through the software vendor) to utilize to determine what specifications are required for each type of electronic transaction.

The implementation guides for the electronic transaction standards (ASC X12N) may be obtained from the Washington Publishing Company, 806 W. Diamond Ave., Suite 400, Gaithersburg, MD, 20878; telephone: 301-949-9740; FAX: 301-949-9742.

Companion Guides

Companion Guides are issued by health care plans to inform and guide the health care provider into compliance with electronic transaction standards and the health plan transaction requirements.

Under the law, health plans are required to accept the standard claim submitted electronically. They may not require providers to make changes or additions to the standard claim. Health plans may not refuse the standard transaction or delay payment of a proper standard transaction.

An additional standard will be adopted for electronic health claims attachments which health plans will be required also to accept. Until that standard is adopted, health plans may continue to require health claim attachments to be submitted on paper. No other additions to standard claims will be acceptable.

HHS has said that **additional information to the standard implementation** guides may be provided within certain limits.

Electronic transactions must go through two levels of scrutiny:

- Compliance with the HIPAA standard. The requirements for compliance must be completely described in the HIPAA implementation guides and may not be modified by the health plans or by the health care providers using the particular transaction.
- Specific processing or adjudication by the particular system reading or writing the standard transaction. Specific processing systems will vary from health plan to health plan, and additional information regarding the processing or adjudication policies of a particular health plan may be helpful to providers.

Such additional information may not be used to modify the standard and may not include:

- Instructions to modify the definition, condition, or use of a data element or segment in the HIPAA standard implementation guide.
- Requests for data elements or segments that are not stipulated in the HIPAA standard implementation guide.
- Requests for codes or data values that are not valid based on the HIPAA standard implementation guide. Such codes or values could be invalid because they are marked not used in the implementation guide or because they are simply not mentioned in the guide.
- Change the meaning or intent of a HIPAA standard implementation guide.

Companion guides can be obtained from each particular health plan.

Implementation of EDI Standards

Providers can achieve TCS/EDI compliance in partnership with business associates (billing services, software venders, clearinghouses, etc.).

They can achieve this compliance in their **internal systems** which requires partnership with their **software vendor(s**). However, because of the interchange of data, HIPAA transaction processing and EDI compliance requires **coordination between all parties: providers, health plans, and clearinghouses.**

The following actions should be taken to accomplish TCS/EDI compliance:

- Identify transactions and code sets currently is use

- Determine HIPAA compliance of current transactions
- Identify information systems and feeder systems
- Determine HIPAA compliance of current systems
- Identify clearinghouse partners
- Determine future relationships
- Determine "clearinghouse to health plan" HIPAA compliance timeframe
- Talk with your venders
- Determine if system modifications (upgrades) are offered
- Determine if new products will be offered
- Talk with your business partners
- Determine their HIPAA compliance plans
- Determine methodology to "secure" business partner relationship
- Involve legal counsel for all contract revision

Within your organization:

- Discuss long term strategic benefits to using additional EDI for your organization
- Analyze cost benefits of potential strategic business changes
- Conduct a HIPAA impact analysis in order to make educated and strategic decisions
- Each system may require more than one change
- One change may impact other systems
- There may be economies of scale with vendors

National Identifiers

Single providers can find themselves with different identifier codes assigned by different health plans, and even within the same health plan. The same identifier may be issued to multiple providers. Millions of employers, often the sponsors of health plans, are subject to similar inconsistencies along with health plans and patients themselves. Employers, providers, payers, clearinghouses, patients and vendors – all participants in health care transactions- must contend with the unnecessary confusion, extra work, processing delays, and high costs created by this lack of standardization.

Health care claims are often delayed or rejected due to processing errors and incorrect coding formats – including incorrect identifier codes for parties to transactions. Some have experienced how non-standard

identifiers have contributed to unethical electronic billing practices and other fraud and abuse in Medicare and in the private health sector.

HIPAA calls for a standard unique health identifier for each individual, employer, health plan, and health care provider for use in the health care system.

The standards for unique identifiers will include:

- National Employer Identifier
- National Provider Identifier
- National Health Plan Identifier
- National Identifier for Individuals

National Employer Identifier (NEI)

Because employers are primary sponsors of health plans, they often must be identified with health care transactions. HHS defines an employer as "a person of entity for whom an individual performs or performed any service, of any nature, as the employee of that person or entity".

The National Employer Identifier (NEI) that has been established by HIPAA law is the unique Employer Identifier Number **(EIN)** assigned to the employer by the Internal Revenue Service. The **compliance date** for the NEI was **July 30, 2004.**

The implementation of the NEI is expected to have a rather mild impact. Examples of the uses of the NEI are:

- Transactions making health plan premium payments to health plans on behalf of employees
- Transactions to other employers as the source or receiver of information about eligibility
- Transactions to enroll or dis-enroll their employees in a health plan

National Provider Identifier (NPI)

The standard unique health identifier is mandated by HIPAA. The NPI is a new number that replaces all "legacy" identifiers that have been used by various health plans. The old "legacy" numbers will no longer be accepted for HIPAA transactions.

All covered entities who are health care providers are eligible for NPIs. They are **required** to obtain and use NPIs. Non-covered providers **may** obtain an NPI if they desire. A payer may require a health care provider who is not considered a covered entity to obtain an NPI. An NPI is expected to last indefinitely, it will not change over time. The NPI is all numeric. It is 10 positions in length (9 plus a check-digit in the

last position). It is easily accommodated in all standard transactions. It contains no embedded information about the provider that it identifies. At the current rate of provider growth, NPIs will be available for 200 years. Providers will be assigned NPIs upon successful completion of an application form. The form can be submitted on paper or over the Internet. Once a provider has been assigned an NPI, the provider must furnish updates to its data within 30 days of any changes. The National Provider System (NPS), built under a CMS contract, will process the applications and updates, ensure the uniqueness of the provider, and generate the NPIs. This rule was finalized on January 23, 2004 and became effective May 23, 2005. The **compliance date was May 23, 2007**.

National Health Plan Identifier

The National Health Plan Identifier standard has not yet been proposed. HHS has stated that it is in the process of development at this time.

National Identifier for Individuals

The standard for the National Identifier for Individuals has been postponed indefinitely and its future is uncertain. Despite the positives of the individual identifier concept, it has generated much public and advocacy group controversy regarding how it can be implemented without compromising individual privacy.

Enforcement of the National Standards

HHS has not simply "suggested" that these Standards be adopted. The law gives the Centers for Medicare and Medicaid Services (CMS) the authority to impose monetary penalties for failure to comply with a standard. HHS is required by statute to impose penalties of not more than $100 per violation on any person or entity who fails to comply with a standard. The total amount imposed on any one person in each calendar year may not exceed $25,000 for violations of one requirement.

Enforcement and Civil Money Penalties (CMP)

This rule establishes rules of procedure for the imposition, by the Secretary of Health and Human Services, of civil money penalties on entities that violate standards adopted by HHS under the HIPAA rules and regulations.

This "Enforcement Rule" sets forth procedural and substantive requirements for imposition of civil money penalties. HHS issued rules of procedure to inform regulated entities of their approach to enforcement and to advise regulated entities of certain procedures that will be followed as they enforce HIPAA.

A business associate is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the business associate, including a workforce member or subcontractor, acting within the scope of the agency.

The Secretary of Health and Human Services has been given the authorization through HIPAA HITECH and the final HIPAA Omnibus Rule to impose civil monetary penalties (CMPs) for violations of the Rules. These penalties apply to medical practices and their business associates. You and your business associates must train your employees to be aware of these penalties so they will know that they are subject to them.

The tiered structure for imposition of CMPs under the HITECH Act and Final Rule distinguishes the level of culpability as follows:

- Unknowing. The covered entity or business associate did not know and reasonably should not have known of the violation. CMP for each violation: **$100 to $50,000**. Total CMP for violation of an identical provision in a calendar year: **$1,500,000**.
- Reasonable Cause. The covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission was a violation, but the covered entity or business associate did not act with willful neglect. CMP for each violation: **$1,000 to $50,000**. Total CMP for violation of an identical provision in a calendar year: **$1,500,000**.
- Willful Neglect – Corrected. The violation was the result of conscious, intentional failure or reckless indifference to fulfill the obligation to comply with HIPAA. However, the covered entity or business associate corrected the violation within 30 days of discovery. CMP for each violation: **$10,000 to $50,000**. Total CMP for violation of an identical provision in a calendar year: **$1,500,000**.
- Willful Neglect – Uncorrected. The violation was the result of conscious, intentional failure or reckless indifference to fulfill the obligation to comply with HIPAA, and the covered entity or business associate did not correct the violation within 30 days of discovery. CMP for each violation: **at least $50,000**. Total CMP for violation of an identical provision in a calendar year: **$1,500,000**.

Under the Final Rule, HHS does not have the authority to automatically impose the maximum CMP for any given violation. Rather, in determining the amount of a CMP, HHS must consider the following:

· The nature and extent of the violation, including the number of individuals affected and the time period during which the violation occurred;

· The nature and extent of the harms resulting from the violation, including whether the violation caused physical harm, whether the violation resulted in financial harm, whether there was harm to an individual's reputation and whether the violation hindered an individual's ability to obtain healthcare;

· The history of prior compliance, including previous violations; and

· The financial condition of the covered entity or business associate, including whether financial difficulties affected the ability to comply and whether the imposition of the CMP would jeopardize the ability of the covered entity to continue to provide or pay for healthcare.

Defenses to CMPs

The Final Rule limits the ability of the Secretary to impose CMPs for certain violations of HIPAA occurring after Feb. 18, 2009. Specifically, the Secretary may not impose CMPs for a violation that is not due to willful neglect and that is corrected within 30 days of actual or constructive knowledge of the violation, or during an additional period, as determined by the Secretary to be appropriate based on the nature and extent of the failure to comply. This defense, however, is not available for violations due to willful neglect. Thus, to the extent possible, a covered entity or business associate that discovers a violation of HIPAA that is not due to willful neglect should endeavor to (i) correct the violation within 30 days of the discovery; (ii) document the date on which it discovered the violations; and (iii) document the date on which it implemented the correction in order to establish a basis for asserting the affirmative defense to the imposition of CMPs for the violation.

The Final Rule also bars the imposition of CMPs for violations of HIPAA when a criminal penalty has previously been imposed for the same conduct.

Enforcement of the HIPAA rules and regulations is assigned to the following agencies within the Department of Health and Human Services.

- Privacy – Office for Civil Rights (OCR)
- Transactions and Code Sets Standards – Office of HIPAA Standards (OHS) through the Centers for Medicare and Medicaid Services (CMS)
- Security – Office of HIPAA Standards (OHS) through the Centers for Medicare and Medicaid Services (CMS)

Privacy Complaints

The Office for Civil Rights (OCR) has stated that they have a legal responsibility to investigate every official privacy complaint they receive. A health care provider may not require individuals to waive their rights to file complaint as a condition of treatment or payment. Any complaints of HIPAA privacy violations are the responsibility of your HIPAA Privacy Compliance Officer.

If a patient comes into your office and wants to file a privacy complaint, follow the steps below:

- The HIPAA Privacy Compliance Officer should formally file the complaint within their office using the Complaint and Resolution form.
- Try to resolve the problem within your office and end the issue there.
- If the patient demands to file a complaint with the government, instruct the patient that he/she will need to contact the OCR (Office for Civil Rights) in writing by either mail, fax, or email (the complaint must be filed within 180 days of when the violation was known, but the OCR may waive this time

limit for "good cause"). If anyone needs help filing a complaint, they can call the OCR at 1-800-368-1019.

Anyone can file written complaints to the OCR by **mail, fax, or email.** Complaints should be sent to the attention of the appropriate OCR Regional Manager **based on the region where the alleged violation took place.**

Full instructions for filing a complaint (including a complaint form) and a list of the Regional offices can be found on the OCR website www.hhs.gov/ocr/privacyhowtofile.htm.

Office for Civil Rights (OCR) Investigations

In order to ensure compliance with the Privacy Rule, OCR has the responsibility to investigate complaints that the Privacy Rule has been violated and to follow up on other information regarding noncompliance.

HHS has given several examples of investigations that may require OCR to have access to PHI:

- Allegations that a covered entity refused to note a request for correction in a patient's medical record, or did not provide complete access to a patient's medical records to that patient.
- Allegations that a covered entity used health information for marketing purposes without first obtaining the individuals' authorization when required by the rule. OCR may need to review information in the marketing department that contains protected health information, to determine whether a violation has occurred.

Make sure that when a patient makes a complaint to your office through your Compliance Officer that it is resolved as quickly as possible. This can prevent any OCR investigations concerning your practice.

Transactions and Code Sets Complaints

The Office of HIPAA Standards (OHS) is responsible for HIPAA transactions and code sets (TCS) enforcement. OHS is an office within the Centers for Medicare and Medicaid Services (CMS), but for purposes of HIPAA enforcement. OHS operates as a separate entity and is completely detached from CMS's Medicare and Medicaid related activities.

To file a complaint, the complainant must provide his\her name and contact information for the organization they represent. They must also provide information about the entity that they are filing a complaint against and the nature of the complaint. OHS will analyze your complaint and send you a status letter within 14 days of receipt of your complaint. You will be contacted if OHS requires additional documentation or information to help resolve the dispute.

The complaint form is provided to assist health care providers to submit written complaints regarding the HIPAA transactions and code sets rule. Filing a complaint with OHS should be a last resort effort to resolve your dispute after working with your trading partners.

You may use the complaint form provided (filled out in its entirety) and mail to the address given.

Breach Notification

Identifying a Breach

The definition of a breach under HIPAA Omnibus means the acquisition, access, use, or disclosure of protected health information in a manner not permitted which compromises the security or privacy of the protected health information.

Breach excludes:

Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted.

Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted.

A disclosure of protected health information where a covered entity 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 such information.

Access, use, or disclosure of protected health information in a manner not permitted is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made.
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary.

When a Breach Occurs

…and identify the affected individuals.

A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.

Breaches treated as discovered. A breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate.

Is patient authorization necessary?

Question: if a device is prescribed for a patient, and that supplier sends us a questionnaire about the use of the device, do we need to get the patient's signed authorization before we return the questionnaire?

Answer: According to the HIPAA Privacy Rule, entities and business associates are permitted to disclose PHI without a signed authorization for treatment, payment, or health care operations reasons. The Privacy Rule requires patient authorization for non TPO (Treatment, Payment, health care Operations). A questionnaire would fall into the TPO category. Returning the questionnaire without patient authorization would be acceptable.

What if PHI is potentially sent to wrong fax number?

Question: One of my staff faxed a referral request containing patient information to a private fax. The recipient called back to inform us the fax was sent to the wrong number. What do I need to do?

Answer: Under HIPAA, faxes and e-mails that contain PHI are allowed for TPO purposes. You need to ensure that the faxes sent from your office for TPO purposes are sent to the correct destination. You must verify the fax number to which you are faxing. It is also recommended that you log your faxes as a good way to track them.

"**These types of disclosures are distinctly different from incidental disclosures. Accidental disclosures happen when a mistake is made in disclosing a patient's PHI. Examples include faxing or mailing PHI to the wrong destination or disclosing PHI to an unauthorized**

person. If you are aware of an accidental disclosure, you need to log the disclosure on the disclosure log. If the disclosure is potentially harmful or damaging to the patient, you need to notify the patient of the accidental disclosure."

Unaccompanied Minors

Question: What is the best policy for unaccompanied minors? What if someone who is not the legal guardian brings a minor in? Should you have that person sign something or do you need written authorization from the legal guardian? Is a verbal authorization to treat okay or must it be written?

Answer: Under the HIPAA Privacy Rule providers are able to treat minor children in emergencies without the parent's consent, but generally the parent still remains the personal representative. The Privacy Rule does not address consent to treatment, nor does it preempt or change State or other laws that address consent to treatment. The Rule addresses access to, and disclosure of, health information, not the underlying treatment. Each state has laws that allow minors to give their own consent for some kinds of health care, such as emergency, general health, contraceptive, and other situations. The HIPAA Privacy Rule defers to state laws. Further, parental consent generally is required for the medical evaluation and treatment of minor children. However, there may be situations when a parent or legal guardian is not available to provide consent.

We would recommend a provider's professional judgment when determining if a minor patient requires treatment or if rescheduling a patient is a better option. Generally a written authorization or consent for treatment is recommended and in our opinion is a best practice. We would recommend the authorization or consent to treat form includes the name and relationship of anyone other than the parent or legal guardian.