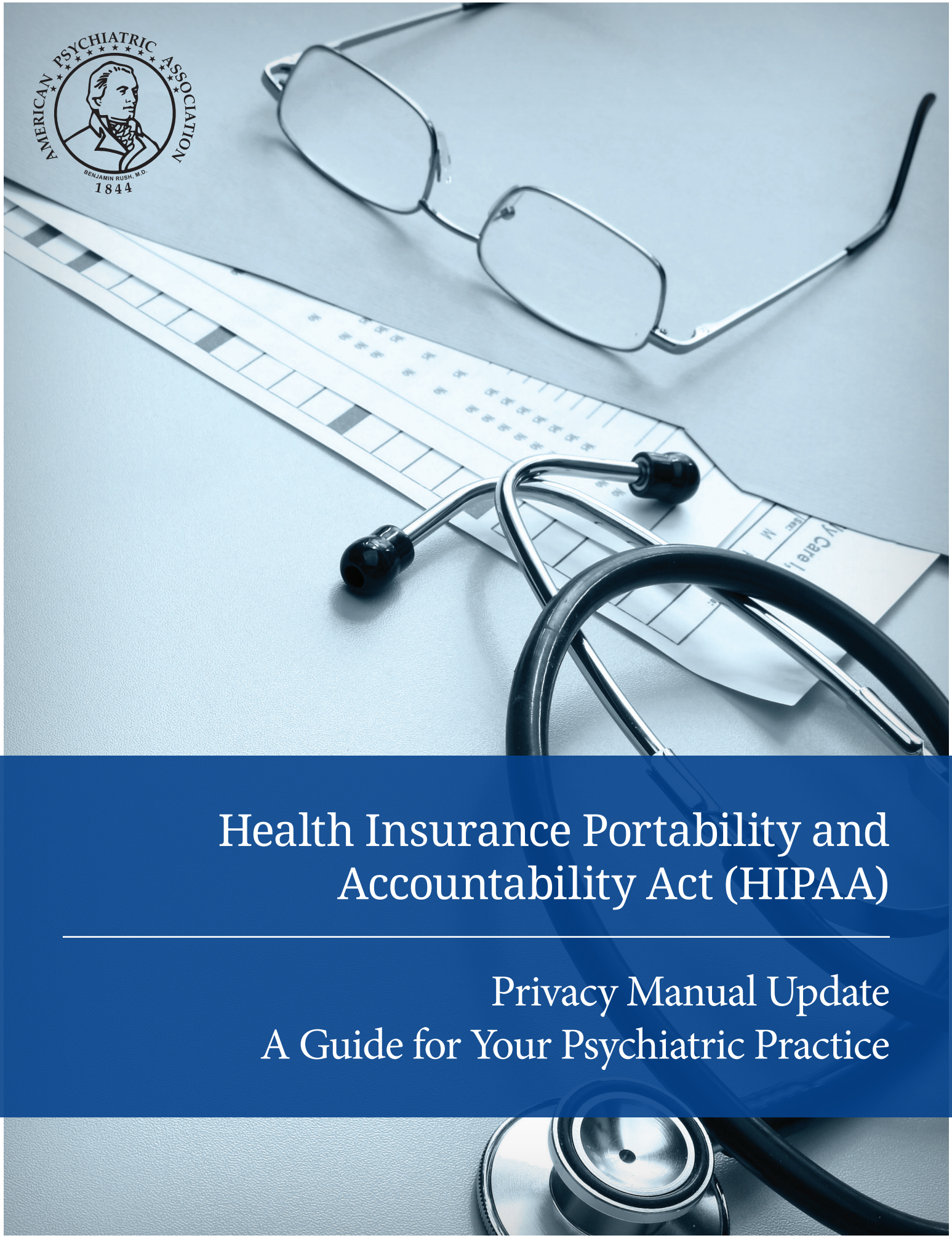

Health Insurance Portability and Accountability Act (HIPAA)

Privacy Manual Update
A Guide for Your Psychiatric Practice

Copyright Notice

For the Manual, generally:

This Manual has been prepared to provide the reader with accurate information on the topics covered in the Manual. The Manual is being provided with the understanding that the American Psychiatric Association and the American Academy of Dermatology Association is not engaged in rendering any legal, accounting or other professional service through this manual. Although the materials contained in the Manual have been written by professionals, the Manual is not intended to be, and should not be used as, a substitute for seeking professional services or advice.

Disclaimer

IMPORTANT DISCLAIMER REGARDING THE LAWS OF YOUR STATE:

Many state privacy laws will continue to apply following the compliance date of the HIPAA privacy regulations. This manual does not include a review of state laws or regulations that may continue to apply after the publication of the HIPAA regulations. The form documents and agreements provided in this manual for your review do NOT necessarily meet the requirements of your state's laws.

You are advised to consult with your state medical society, local chapter of specialty society, legal counsel or advisors familiar with your state's laws to determine which state laws and regulations will impact: (1) the operation of your practice, and (2) the contents of any form, template document or agreement contained in this manual.

IMPORTANT DISCLAIMER REGARDING THE USE OF THIS MANUAL:

THIS MANUAL IS NOT INTENDED AS, AND DOES NOT CONSTITUTE, LEGAL OR OTHER PROFESSIONAL ADVICE. This publication is distributed with the understanding that American Psychiatric Association and the American Academy of Dermatology Association and the manual's contributors are not engaged in rendering financial, legal, or other professional advice through this manual. The American Psychiatric Association and the American Academy of Dermatology Association and the manual's contributors have used their best skills to ensure that the contents of the manual are accurate; however, the information contained in this Health Insurance Portability and Accountability Act (HIPAA) Privacy Manual: A How to Guide for Your Medical Practice is for informational purposes only.

This manual should be used only as a general reference and guide for outlining specific steps that you may take in order to comply with certain regulations issued pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The steps contained in this manual are general examples and should serve only as suggested starting points in your practice's compliance with HIPAA. You may desire to alter the formatting, typeset, organization and fonts size of the manual as long as the integrity or substance of the manual is maintained.

THE AMERICAN PSYCHIATRIC ASSOCITION AND THE AMERICAN ACADEMY OF DERMATOLOGY ASSOCIATION ARE NOT RESPONSIBLE FOR, AND WILL NOT BE LIABLE FOR, ANY DAMAGES YOUR PRACTICE MIGHT INCUR THAT ARE ASSOCIATED WITH YOUR USE OF THIS MANUAL OR ITS CONTENTS (INCLUDING ANY FORMS, TEMPLATE DOCUMENTS OR AGREEMENTS). If you require legal or other professional advice, you should consult a professional skilled in that area.

2013 Update by: Health Care Law Associates, P.C. www.thehealthcaregroup.com

Contents

Introduction to the Health Insurance Portability and Accountability (HIPAA) Manual

Patients want to trust that the healthcare system will keep their personal health information private. The passage of the Health Insurance Portability and Accountability Act (HIPAA) in August 1996 gave the federal government the ability to mandate how healthcare plans, providers, and clearinghouses store and transmit individuals' personal information as it relates to the administration, provision and payment of healthcare. Your practice needs to be aware of and be prepared to implement the HIPAA Privacy and Security Rules. These two rules fall under one of the general categories of HIPAA known as the Administrative Simplification Act. The Privacy and Security Rules underwent substantial modification as result of the passage of Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (commonly known as the "Health Information Technology Act for Economic and Clinical Health" or "HITECH").

Until the passage of HIPAA and the promulgation of the Privacy and Security Rules, there had been no national or industry standard governing the privacy and security of an individual's health information. Developments in technology and the ability to gain easy access to personal health information drove efforts to streamline diverse state regulations and insurance company requirements into a single regulation. The passage of HIPAA and HITECH occurred, in part, to improve the efficiency and effectiveness of the healthcare system by standardizing the transmission of certain administrative and financial transactions and by protecting the privacy and security of personal health information.

The Privacy Rule essentially controls the use and disclosure of what is known as protected health information (PHI). Many of the applications of the Privacy Rule are simply common sense. Others are somewhat more complex and actually afford the patient a great deal of flexibility in the knowledge of the content of their medical record and how that content (PHI) is used. As well, the Rule enables the patient to control the disclosure of their protected health information to certain entities.

The Security Rule focuses on the ability of covered entities (including medical practices) to protect and safeguard the confidentiality of medical information. The Security Rule is similar in nature to the Privacy Rule; however it is more complex in terms of its impact on medical practices in areas specific to the transmission, storage and receipt of data. In particular, the practice's computer network, access to it and the method by which the practice stores and handles data come under close scrutiny.

There are many resources currently available that address HIPAA and how it will affect healthcare. However, few if any, address the regulation as it directly relates to medical practices. This manual is written specifically for medical practices.

In addition to generally explaining these regulations, this manual will provide your practice with an overview and a step-by-step approach to understanding, implementing and complying with the HIPAA Privacy Rule.

To facilitate compliance with the Privacy Rule, this manual includes detailed checklists, "how to" guides and sample documents to ensure compliance with HIPAA. Implementation of the Minimum Necessary standard, as explained herein, will vary from practice to practice. For those unfamiliar with the term Minimum Necessary, it is the principle that individually identifiable health information should only be disclosed to the extent needed to support the intended purpose of the disclosure of the information for treatment. Therefore, what may be reasonable to implement in one practice may not be reasonable in another. Every effort should be made to adhere to the minimum necessary standard by limiting the uses and disclosures of protected health information within the practice.

How To Use This Manual

◆ The overview and the glossary can be copied and shared with all staff (including physicians) as a training tool.

◆ Following the overview are individual steps that should be followed to achieve compliance with the Privacy Rule.

◆ The To Do notice on each page provides suggestions for meeting the Privacy Rule Requirements.

◆ The Note notice cautions, observations and recommendations that will further guide your practice to HIPAA compliance.

◆ The Internal Privacy Checklist provides useful, practical insight into HIPAA and the more general confidentiality practices to apply within your practice.

◆ The section of Exhibits provides all of the necessary forms and other documents that you will need to implement HIPAA in your practice.

◆ Please note that your Privacy Officer or a designated staff member will need to fill in your practice's name on each Exhibit if you wish to convert the manual into your practice's privacy compliance plan and record.

◆ The Appendix section provides helpful resources to assist your practice in becoming compliant with HIPAA. The Exhibit and Appendix sections also contain psychiatry specific materials and references.

This manual does NOT include such items as training materials, specific procedures, state specific information, or HIPAA's special research requirements.

A HIPAA Glossary

This glossary is an overview. The items herein are discussed in further detail in the following steps.

Authorization Form

A form that a healthcare provider must obtain from the individual patient or patient guardian in order to use or disclose the individual's protected health information (PHI) for purposes other than for treatment, payment, and healthcare operations (TPO) or for specific purposes listed in the Privacy Rule, such as public health or health oversight.

Business Associate

A person or entity that is not a member of your practice's workforce who uses or discloses PHI to carry out certain functions or activities on behalf of the medical practice or other covered entity.

Breach

Acquisition, access, use or disclosure of PHI in a manner not permitted by HIPAA which compromises the security or privacy of such information.

Consent Form

A form that a healthcare provider having a direct treatment relationship with an individual may obtain from the individual in order to use or disclose the individual's protected health information (PHI) for treatment, payment and healthcare operations (TPO). USE OF THIS FORM IS OPTIONAL AND NOT REQUIRED UNDER HIPAA.

Covered Entity

Under HIPAA, this means health plans, healthcare clearinghouses and any healthcare providers (physicians, hospitals, nursing homes, etc.) who transmit any health information in electronic form in connection with a HIPAA transaction.

Data Use Agreement

An agreement that sets forth the permitted uses and disclosures of limited data sets, including who may use or receive the data and limitations on the receiving party's ability to re-identify or contact the individuals who are subjects of the limited data sets.

Department of Health and Human Services (HHS)

A department of the executive branch of the federal government that has overall responsibility for implementing HIPAA.

Designated Record Set

A group of records maintained by or for a covered entity. That is:

◆ the medical records and billing records about individuals maintained by or for a covered healthcare provider;

◆ the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

◆ used, in whole or in part, by or for the covered entity to make decisions about individuals.

Direct Treatment Relationship

A treatment relationship between an individual and a healthcare provider in which the provider delivers healthcare directly to an individual rather than through another healthcare provider. (See "Indirect Treatment Relationship" definition.)

Disclosure

The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Disclosure History

Under HIPAA this is a list of any entities that have received personally identifiable healthcare information for uses unrelated to treatment, payment and healthcare operations (TPO).

Electronic Health Record

Electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff.

Federal Privacy Act of 1974

This Act protects personal information about individuals held by the federal government. Covered entities that are federal agencies or federal contractors that maintain records that are covered by the Privacy Act not only must comply with the Privacy Rule's requirements but also must comply with the Privacy Act.

Health Information

Any information created or received by a provider that relates to the past, present, or future physical or mental health condition of a patient, or the past, present or future payment for the provision of healthcare to a patient, or the provision of healthcare to a patient.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

A federal law that allows persons to qualify immediately for comparable health insurance coverage when they change their employment relationships. Title II, Subtitle F of HIPAA gives the Department of Health and Human Services (HHS) the authority to mandate the use of standards for the electronic exchange of healthcare data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for healthcare patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable healthcare information.

Health Plan

An individual or group plan that provides, or pays the cost of, medical care.

Healthcare

Healthcare includes, but is not limited to, the following:

Preventive, diagnostic, therapeutic, rehabilitative maintenance, or palliative care, and counseling service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Healthcare Clearinghouse

Under HIPAA, this is an entity that processes or facilitates the processing of information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction, or that receives a standard transaction from another entity and processes or facilitates the processing of that information into nonstandard format or nonstandard data content for a receiving entity.

Healthcare Operations

Activities related to your practice's business, clinical management and administrative duties. Some examples of these activities are use of PHI to obtain a referral, quality assurance, quality improvement, case management, training programs, licensing, credentialing, certification, accreditation, compliance programs, business management and general administrative activities of the practice. Healthcare operations is further defined to include all activities associated with the selling, merging, transferring or consolidation of medical practices and other covered entities.

Healthcare Provider

A person or organization that provides, bills and is paid for healthcare services.

Incidental Use or Disclosure

Is defined by the Privacy Rule "as a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure."

Indirect Treatment Relationship

A relationship between an individual and a healthcare provider in which:

◆ The healthcare provider delivers healthcare to the individual based on the orders of another healthcare provider; and

◆ The healthcare provider typically provides services or products, or reports the diagnosis or results associated with the healthcare that they have recorded or provided directly to another healthcare provider who provides the services or products or reports to the individual.

Individually Identifiable Health Information (IIHI)

Any health information (including demographic information) that is collected from the patient and:

◆ is created or received by a healthcare provider or other covered entity or employer; and

◆ that relates to the past, present or future physical or mental health or condition of an individual; OR the provision of healthcare to an individual, or the past, present or future payment for the provision of healthcare at your practice; AND that could potentially identify an individual.

Limited Data Set

PHI that excludes specific, readily identifiable information about the individual patients as well as their relatives, employers and members of their households. The Limited Data Set may include admission, discharge and service dates; date of death; age (including ages 90 and over) and any geographic subdivision (including town or city, state and five digit zip code, but excluding postal addresses).

Marketing

"To make a communication about a product or service, that encourages the recipients of the communication to purchase or use the product or service."

Minimum Necessary

In regard to HIPAA, the principle that, to the extent practical, individually identifiable health information (IIHI) should only be disclosed to the extent needed to support the intended purpose of the disclosure of the information for treatment.

Notice of Privacy Practices

A document that health care providers and other covered entities must develop in order to inform patients about their rights surrounding the protection of their PHI.

Office of Civil Rights (OCR)

The HHS sub department responsible for the enforcement of the HIPAA privacy rules.

Operations

See Healthcare Operations.

Payer

In healthcare, an entity that assumes the risk of paying for medical treatments. This can be an uninsured patient, a self-insured employer, a health plan or an HMO (also payor).

Payment

The activities by the practice to obtain reimbursement for healthcare services. This includes, among others, billing, claims management, collection activities, verification of insurance coverage and precertification of services.

Personal Representative

A person who, under applicable law, has the authority to act on behalf of an individual in making decisions related to healthcare.

Protected Health Information (PHI)

With few exceptions, includes individually identifiable health information (IIHI) held or disclosed by a practice regardless of how it is communicated (e.g., electronically, verbally, or written).

Psychotherapy Notes

Notes recorded (in any medium) by a healthcare provider who is a mental health professional documenting or analyzing the contents of conversation 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, counseling session start and stop times, 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. See Exhibit 26 for more information on psychotherapy notes.

Third-Party Administrator (TPA)

An entity that processes healthcare claims and performs related business functions for a health plan.

Treatment

The provision, coordination or management of healthcare and related services by one or more healthcare providers; or the referral of a patient for healthcare from one provider to another.

Workforce

Under HIPAA, this means employees, volunteers, trainers, and other persons under the direct control of a covered entity, whether or not they are paid by the covered entity.

Unsecured PHI

PHI that is not secured through the use of a technology standard that renders it unusable, unreadable or indecipherable to unauthorized individuals through the use of encryption or destruction, which are the technologies or methodologies specified by the Secretary of HHS.

Use

With respect to individually identifiable health information (IIHI), the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Step-By-Step Guide to the Privacy Rule

In order to ensure compliance with the Privacy Rule, this list of tasks should be completed. The step-by-step instructions for each of these tasks are included in this manual. Check off each task as it is completed to make sure that each task is completed. It is not necessary to complete these tasks in the order that they are listed. You may find it helpful to do certain tasks before others.

Date Reference

✔ Completed

_____ _____ Read the Overview of the Privacy Rule

_____ _____ Select a Privacy Officer

_____ _____ Review and Implement Privacy Officer Responsibilities

_____ _____ Conduct a Walk-Through of the Practice to Identify Privacy Risk Areas

_____ _____ Implement a Notice of Privacy Practices

_____ _____ Implement a Written Acknowledgement Process

_____ _____ Implement Privacy Policies and Procedures

_____ _____ Implement Patient Authorization Form

_____ _____ Implement a Form Requesting Restrictions on Uses and Disclosures of PHI

_____ _____ Receipt of Requests for Confidential Communications of PHI

_____ _____ Implement a Form to Inspect and Copy PHI

_____ _____ Implement Access Denial Form

_____ _____ Implement a Form to Amend PHI

_____ _____ Implement a Form to Receive an Accounting of Certain Disclosures of PHI

Date	Reference	✔ Completed
_____	_____	Implement a Log to Track Disclosures of PHI
_____	_____	Implement Patient Complaint Forms
_____	_____	Determine Who Can Use and Disclose PHI
_____	_____	Update or Develop Job Descriptions with Respect to PHI Use and Disclosure
_____	_____	Develop a List of Your Business Associates
_____	_____	Implement Business Associate Agreements
_____	_____	Train All Physicians and Staff on the Privacy Policies and Notice of Privacy Practices
_____	_____	Document Physician and Staff Training
_____	_____	Obtain Signed Workforce Confidentiality Agreements from All Physicians and Staff
_____	_____	Monitor Compliance with the Privacy Rule
_____	_____	Breach Notification Requirements

Step 1: Read the Overview of the Privacy Rule

Covered Entities/Providers

Covered Entities, are required by law to be compliant with the Privacy Regulations promulgated under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as further modified by the Health Information Technology for Economic and Clinical Health Act (HITECH).

WHAT IS A COVERED ENTITY?

A covered entity means a health plan or payor (including government payors), a healthcare clearinghouse (such as an organization or billing service that processes health information into or out of standard format), or a healthcare provider such as a physician, hospital or pharmacy.

• For the purposes of this manual, all healthcare providers who transmit any healthcare information in electronic form are considered covered entities.

There are three main purposes to the Privacy Rule as stated by the Department of Health and Human Services.

First Purpose

To protect the rights of patients by providing them access to their protected health information (PHI) and the ability to control the use and disclosure of their PHI.

Second Purpose

To restore the public's trust in the healthcare delivery system.

Third Purpose

To improve the efficiency and effectiveness of healthcare delivery in the United States by creating a national framework for healthcare privacy.

The Privacy Rule provides protection for patients' health information. In the past, patients had no standardized legal protection for the privacy of their medical records. Now, with continued advances in electronic technology including the Internet, there is growing concern among the public, as expressed by certain political leaders, regarding the confidentiality of individually identifiable health information.

Protected Health Information

WHAT IS PHI?

Protected health information (PHI), with few exceptions, includes individually identifiable health information (IIHI) held or disclosed by a practice regardless of how it is communicated (e.g., electronically, verbally or written).

Individually Identifiable Health Information

WHAT IS IIHI?

The term individually identifiable health information (IIHI) means any health information (including demographic information) that is collected from the patient or created or received by a healthcare provider or other covered entity or employer that relates to:

the past, present or future physical or mental health or condition of an individual

OR

the provision of healthcare

OR

the past, present or future payment for the provision of healthcare by your practice

AND

that either actually or reasonably could identify an individual.

The Privacy Rule considers 18 items that could be used to identify a patient. They are:

Identifiable Information

1. Name
2. Any address specification such as street, city, county, precinct, and zip code*
3. All dates except for the year including birthdate, admission date, discharge date, date of death and all ages over 89
4. Telephone number
5. Fax number
6. Electronic mail address
7. Social Security number
8. Medical record number
9. Health plan beneficiary number
10. Account number maintained by the healthcare provider
11. Certificate or license number such as driver's license number
12. Vehicle identifier and serial number including license plate number
13. Medical device identifier and serial number such as pace maker serial number
14. Web site address
15. Internet protocol (IP) address number
16. Biometric identifier including finger and voice prints
17. Full-face photographic images and any comparable image, and
18. Any other unique identifying number characteristic or code.

*Entire zip code must be removed if the geographic unit formed by combining all zip codes with the same three initial digits has a population of < 20,000 people; otherwise only the last two digits must be removed.

WHAT IS DE-IDENTIFIED DATA?

IIHI is considered de-identified

1. if the 18 aforementioned items are removed from the information, or
2. if a statistician or similarly experienced person determines that there is a very small risk of re-identifying the information and he/she documents his/her findings.

Many covered entities require the use of PHI that is not completely de-identified for certain activities. As a result, uses and disclosures of a limited data set are permitted, as long as they are used for research, public health, and health care operations purposes only.

WHAT IS A LIMITED DATA SET?

A **Limited Data Set** is PHI that excludes specific, readily identifiable information about the individual patients as well as their relatives, employers and members of their households. Sixteen of the 18 aforementioned items must be removed from the limited data set. The items that can remain are date references [e.g., admission, discharge and service dates; date of death; age (including age 90 and over)], and any geographic subdivision (including town or city, state or five-digit zip codes), but excluding postal addresses.

Covered entities that choose to use a Limited Data Set must obtain a Data Use Agreement from the persons who will be using the information contained in the data set. HHS does not specify a specific format for the Data Use Agreement other than requiring the following items be included:

- the permitted uses and disclosures of the data by the recipients,
- a description of who can use or receive the data, and
- a statement that the recipient of the information is to agree not to: (i) use or further disclose the information other than as permitted by the Data Use Agreement or by law; (ii) use appropriate safeguards to prevent disclosure of the information other than as provided in the Data Use Agreement; (iii) report to the covered entity any use or disclosure of the information not provided for by the Data Use Agreement of which the recipient becomes aware; and (iv) re-identify the information or contact the individuals.

Therefore, covered entities can choose whatever format for the Data Use Agreement that best suits their organization. For example, covered entities could simply use the confidentiality agreement that is found in Exhibit 20, or a Business Associates Agreement, or other formal agreement, provided that it is revised to include the requirements listed above. The terms of the agreement can be customized to suit the needs of the covered entity.

Patient Control Over Health Information

One of the major purposes of the Privacy Rule is to provide patients access to their medical records. Ultimately through this Rule, patients can control who has access to their medical record and PHI. Generally, under the Privacy Rule, healthcare providers have the right to use and disclose PHI about a patient in order to carry out the treatment, payment or healthcare operations (referred to as TPO) of that provider's practice. This right to use and disclose PHI is valid as long as the provider makes a good faith effort to obtain written acknowledgment from the patient that he/she has received a copy of the Notice of Privacy Practices. Additionally, healthcare providers may disclose PHI to other healthcare providers for the treatment activities of that provider, and may disclose PHI for the payment activities and certain operational activities (e.g., quality assurance of other covered entities) of that other healthcare provider.

Practices must grant a patient's request for restriction on disclosures if the disclosure is for payment or health care operations and if the PHI pertains to a service for which the patient paid in full, out of pocket. This restriction on disclosure does not apply when the disclosure is made for treatment purposes.

WHAT IS TPO?

TPO refers to the treatment, payment or healthcare operations of a practice.

T: Treatment means the provision, coordination or management of healthcare and related services by one or more healthcare providers or the referral of a patient for healthcare from one provider to another.

P: Payment means the activities conducted by the practice to obtain reimbursement for healthcare services. This includes, among others, billing, claims management, collection activities, verification of insurance coverage, and precertification of services.

O: Healthcare Operations means activities related to your practice's business and clinical management and administrative duties. Some examples of these activities are quality assurance, quality improvement, case management, training programs, licensing, credentialing, certification, accreditation, compliance programs, business management and general administrative activities of the practice. Healthcare Operations is further defined to include all activities associated with the selling, merging, transferring or consolidation of medical practices and other covered entities.

Generally speaking, prior to the Privacy Rule, patients did not have the right to limit or restrict the amount of information that was disclosed to carry out TPO. Under certain circumstances, the Privacy Rule allows patients the right to request restriction(s) on uses or disclosures of their PHI for TPO. Patients must be informed of their rights to request such restriction(s) to their records; however, the provider is not required to agree to the restriction. If the provider agrees to a restriction(s), it must document the restriction(s) and must abide by the restriction(s) unless there is an emergency and the restricted PHI is necessary to provide emergency treatment. In an emergency, the healthcare provider providing treatment cannot disclose the restricted information beyond the emergency treatment situation.

A patient-requested restriction on PHI may be terminated by the practice if:

1. The patient agrees to or requests the termination in writing;

2. The patient orally agrees to such termination and the oral agreement is documented;

3. The practice informs the patient that it is terminating the restriction (such a termination is only effective against PHI created or received after the date of termination).

Confidentiality

In addition to patient-imposed restrictions on PHI, the practice must allow patients to request that communications regarding PHI be delivered by alternative means (e.g., in person rather than by mail) or in alternative locations (e.g., different addresses). The practice must accommodate reasonable requests of such confidential communications. However, the practice may require the patient to make such a request in writing and may condition the accommodation on information as to payment mechanisms, if any, and an alternative address or other contact method. The practice may not condition the confidential communication on receiving an explanation from the patient as to the basis for such a request.

Limitations of Use And Disclosure of PHI

The Privacy Rule limits the use and disclosure of a patient's PHI. The Privacy Rule generally requires medical practices to take reasonable steps to limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose. For example, a medical practice may limit access to the medical record only to the physicians, nurses and other clinical personnel within the practice who need access to it to provide clinical care.

WHAT DOES "USE" MEAN?

Use means the sharing, employment, application, utilization, examination or analysis of PHI within the practice.

WHAT DOES "DISCLOSURE" MEAN?

Disclosure means the release, transfer, giving access to or divulging in any other manner of PHI to anyone outside of the practice.

WHAT IS MINIMUM NECESSARY?

Minimum Necessary is a standard requiring covered entities to limit the amount of PHI that is used or disclosed to the "minimum necessary" to accomplish the intended purpose unless the disclosure is to the patient, the Secretary of the Department of Health and Human Services, or to another provider for treatment purposes.

The Minimum Necessary Standard

Covered entities must make reasonable efforts to use or disclose, or to request from another covered entity, only the minimum amount of PHI required to achieve the purpose of the particular use or disclosure. The Privacy Rule requires that covered entities implement policies and procedures to ensure "minimum necessary" uses and disclosures.

Specifically, every covered entity (practice) is required to implement policies and procedures to identify:

(i) the persons or classes of persons in its workforce who need access to PHI to carry out their duties; (ii) the category or categories of PHI to which such persons or classes need access; and (iii) the conditions that would apply to such access. Furthermore, covered entities must implement policies and procedures that limit access to only these identified persons, and only to the identified PHI. Covered entities, including healthcare providers, should not grant access to PHI to individuals or organizations that do not need access in order to perform a service on behalf of the covered entity. In other words, you should not grant anyone access to PHI who does not need access to perform a service for you. Please realize, many other individuals and organizations might have access to your offices (for example, a security

guard, or a janitor). To prevent a violation of the privacy rule from occurring due to a disclosure to a non-business associate, the practice can take the following actions:

1. First, the practice must recognize that it has an obligation to implement reasonable administrative, physical and technical safeguards to protect PHI from such unauthorized access. In other words, a security guard or janitor should not be able to easily view PHI (for example, open charts or lists of patient names with lab results);

2. As stated above, the practice should implement policies to prevent such unauthorized disclosure/access. Furthermore, the practice should educate its workforce and applicable third parties (the security company, the janitorial service, etc.) about the policies. The practice might even provide a copy of its policies to those individuals and/or companies to make them aware that they should not access or attempt to access unauthorized information; **and**

3. Consider requiring non-business associates that might have access to your offices to sign a confidentiality agreement, agreeing that: (i) the party will not access or attempt to access PHI; and (ii) if PHI is accessed (accidentally or otherwise), the individual or entity will not use or further disclose the PHI.

It is acknowledged that implementation of the Privacy Rule will vary from practice to practice. ***For example, it may be necessary for staff of smaller practices to have access to all PHI in order to carry out their job responsibilities. On the other hand in a larger practice, the receptionist or phone operator may not need access to a patient's chart, and thus their "minimum necessary" would be significantly different.*** Every effort should be made to adhere to the minimum necessary standard by limiting the uses and disclosures of PHI within the practice. <u>For further discussion as to what the minimum necessary standard means for psychiatric practices, please see Exhibit 25 for the American Psychiatric Association's position statement.</u>

Regarding disclosures of PHI, non-routine disclosures (i.e., outside the ordinary course of business) should be reviewed on a case-by-case basis to ensure that only the minimum necessary information is released. For routine disclosures (e.g., the filing of claims with an insurer), covered entities must implement policies and procedures that permit only the disclosure of the minimum PHI reasonably necessary to achieve the purpose of the disclosure. Again, such policies must identify the types of PHI to be disclosed, the types of persons who would receive the PHI, and the conditions that would apply to such access.

A VERY IMPORTANT NOTE

According to the Privacy Rule, a case-by-case review of each request for an entire medical record is not required if the record is being disclosed for treatment purposes (e.g., the record is released to another practice for continued treatment). The minimum necessary requirement is not meant to keep the practice from performing its daily clinical functions. Medical practices should feel free to engage in whatever communications are required for quick effective and high quality patient care so long as every effort is made to comply with the Privacy Rule and to maintain patient privacy. To this end, medical

practices are entitled to make their own assessment of what PHI is necessary to treat each patient and to implement policies and procedures accordingly.

WHAT ARE THE EXCEPTIONS TO THE MINIMUM NECESSARY STANDARD?

- The request by a healthcare provider to use and receive the information for treatment purposes, such as in the case where a patient has been referred to another provider for a consultation.
- Disclosure to the patient who is the subject of the information.
- When the patient has signed an authorization for the practice to release the PHI to a third party, such as an employer or life insurance company.
- Any disclosures that the Department of Health and Human Services (DHHS) requires under the Privacy Rule for enforcement purposes.
- Any uses or disclosures that are required by any other law, such as a police investigation.
- Uses and disclosures required for compliance with the HIPAA transaction standards.

Notice of Privacy Practices and Acknowledgment

The Privacy Rule allows medical practices and other covered entities to use and disclose PHI for treatment, payment and healthcare operations ("TPO") without obtaining the patient's written authorization. However, medical practices and other covered entities with direct treatment relationships must provide the patient with the Notice of Privacy Practices for PHI and use best efforts to obtain the patient's written acknowledgment of receipt of the Notice.

WHAT IS A NOTICE OF PRIVACY PRACTICES?

A document that health care providers and other covered entities must develop in order to inform patients about their rights surrounding the protection of their PHI.

The patient's written acknowledgment of receipt of the Notice of Privacy Practices must be obtained on the date the first service is rendered to the patient.

◆ However, a practice is NOT required to obtain the patient's written acknowledgment of receipt of the Notice of Privacy Practices under the following circumstances in the event of an emergency; though the practice must use reasonable efforts to obtain such acknowledgment as soon as reasonably practicable after the emergency.

◆ If a patient refuses to sign the acknowledgment and the practice documents such refusal. If written acknowledgement of the receipt of the Notice of Privacy Practices is not obtained, then the practice must document its efforts to do so. The practice may not deny medical treatment for failure to sign an acknowledgment of receipt of the Notice of Privacy Practices. The practice may use and disclose the patient's PHI in accordance with the Privacy Rule and state law regardless of the patient's refusal to sign an acknowledgment.

The Privacy Rule requires only that the acknowledgement be in writing and does not specify the format that covered entities are to use to obtain the acknowledgement. Covered entities may, for example, have patients sign a separate sheet, or simply initial a cover sheet of the Notice of Privacy Practices to be retained by the practice.

Use of PHI for TPO and Non-TPO Purposes

A practice may only use and disclose protected health information ("PHI") without a written patient authorization, or as otherwise permitted or required by law, as follows:

- For its own treatment, payment and health care operations purposes;
- For the treatment activities of any health care provider;
- For the payment activities of another covered entity or any health care provider;
- For the health care operations activities of another covered entity if each entity either has or had a relationship with the individual who is the subject of the PHI, and (i) the purpose of the disclosure relates directly to certain limited types of health care operations (described in the text box "Permissible Disclosures to Another Covered Entity for Certain Health Care Operations") and the PHI pertains to such relationship, or (ii) for the purpose of healthcare fraud and abuse detection or compliance; and
- For any health care operations activities of an organized healthcare arrangement in which the disclosing covered entity participates.

WHAT IS AN AUTHORIZATION?
A healthcare provider must obtain written permission; or authorization, as it is referred to in the HIPAA Privacy Rule, to use or disclose the individual's PHI for purposes other than for TPO. The authorization must describe the specific use or uses of the information, to whom it will be disclosed, and include an expiration date for the disclosure.

An Authorization gives medical practices and other covered entities permission to use or disclose specified PHI for specific purposes other than for TPO, such as disclosure of PHI to a third party specified by the patient, such as to a life insurance company in order to obtain life insurance.

WHAT ARE PERMISSIBLE DISCLOSURES TO ANOTHER COVERED ENTITY FOR CERTAIN HEALTH CARE OPERATIONS?
Practices may disclose PHI to other covered entities for that covered entity's health care operations, to the extent that the patient has a relationship with the individual who is the subject of the PHI and under the following health care operations:

- quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities;
- population-based activities related to improving health or reducing health care costs, protocol development, case management, care coordination, contacting of health care providers and patients with information about treatment alternatives;

continued

- related quality assessment functions that do not include treatment;
- review of the competence or qualifications of health care professionals;
- evaluation of practitioner and provider performance and health plan performance;
- training programs in which students, trainees or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers;
- training non-health care professionals;
- accreditation, certification and licensing activities;
- credentialing activities; and
- for the purpose of health care fraud and abuse detection or compliance.

Note!!
IMPORTANT:
In almost all instances, the Privacy Rule requires providers to obtain Authorization to use or disclose PHI maintained in psychotherapy notes. For further discussion on psychotherapy notes, please see the American Psychiatric Association's resource documents found at Exhibit 26. Additionally, this general rule regarding the need for authorizations prior to the disclosure of psychotherapy records must be balanced against the facts and circumstances of the situation. For example, exceptions to the authorization requirement exist in situations where a patient is deemed to present a serious danger to themselves or others. See Exhibit 27 for additional discussion from the Secretary of HHS.

At a minimum, Authorizations must:

◆ contain a specific expiration date that relates to the patient or the purpose of the use or disclosure (except for those authorizations related to research, which must post either an expiration date/event, or a statement that no such expiration date/event exists);

◆ name the person/entity authorized to make the requested use or disclosure (for example, the practice);

◆ name the person/entity authorized to receive the PHI from the medical practice;

◆ describe the PHI to be used or disclosed;

◆ include a description of each purpose of the use or disclosure;

◆ inform the patient of his/her right to revoke the Authorization, including exceptions to this right and a description of how to revoke the Authorization;

◆ for sales of PHI, include a statement that the disclosure will result in remuneration for the practice;

◆ warn the individual that additional disclosures may occur and that the PHI may no longer be protected by the Privacy Rule;

- include a statement that treatment may not be conditioned on receipt of the authorization, or under the circumstances where it can be conditioned such as for research purposes,

a statement about the consequences of refusing to sign the authorization;

- be signed by the patient or his/her personal representative; and
- if signed by a personal representative, a description of his/her authority to act for the individual.

Though all patient authorizations will contain the standard elements noted above, some may vary depending on the purpose of the disclosure.

A covered entity will need three (3) basic forms of authorization:

1. **Authorizations on which treatment may not be conditioned.** These authorizations must contain all of the standard elements listed above. The practice must treat the patient even if he or she refuses to sign the authorization.

2. **Authorizations on which treatment may be conditioned (e.g., authorizations for occupational health screenings or instances where the treatment is incident to research**). The authorization must clearly state the consequences of the individual's refusal to sign the authorization (e.g., that the practice may withhold treatment if the patient does not sign the authorization.). See Appendix 7 for additional information regarding research — specific authorizations.

3. **Authorizations for marketing purposes (unless the communication is during face-to-face with a patient; or a promotional gift of nominal value**). The authorization must contain all of the standard elements noted above. In addition, if the marketing involves direct or indirect remuneration to the practice by a third party, the authorization must include such a statement (though the authorization does not need to disclose the amount or type of remuneration).

In all instances, you must provide the individual with a copy of his/her signed authorization.

Authorizations are required by HIPAA to be retained by your practice for a minimum of six (6) years. Please review your state's laws concerning retention of medical records to determine if any stricter standards apply.

Business Associates

Many physician practices require assistance from outside entities to accomplish some or all of their business activities and functions. For example, billing and collection, marketing and technology services. Many of these types of entities may be identified under the Privacy Rule as "Business Associates."

WHAT IS A BUSINESS ASSOCIATE?

A person or entity that is not a member of your practice's workforce who uses or discloses PHI to carry out certain functions or activities on behalf of the medical practice or other covered entity.

Business Associates are required under HIPAA to comply with certain aspects of the Privacy and Security Rules. HIPAA requires a written Business Associate Agreement between a practice and its Business Associates, and a similar agreement between a practice's Business Associates and such Business Associates' subcontractors. See Exhibit 15 for a list of sample Business Associates and Exhibit 16 for a flow chart to help identify Business Associates specific to your practice. Keep in mind that a Business Associate is a party whose relationship with the practice requires access and/or use of PHI. For example, most of the pharmaceutical representatives should not need access to your practice's PHI, and would not be considered Business Associates. The final determination of who is and who is not a Business Associate will vary among medical practices. Who may be a Business Associate for one practice may not be a Business Associate for another medical practice.

Once your practice's Business Associates are identified, the Privacy Rule requires that the practice execute a Business Associate Agreement with each Business Associate prior to the use or disclosure of PHI. See Exhibit 17 for a sample Business Associate Agreement.

A Business Associate Agreement is not necessary for a Covered Entity who discloses PHI to a healthcare provider for treatment purposes. For example, PHI exchanged between a hospital and a physician with admitting privileges at the hospital does not require a Business Associate Agreement. In addition, direct and indirect providers who are providing treatment to a patient are not Business Associates. ***An example is when the radiologist reads the patient's x-rays for the medical practice, but never sees the patient face-to-face, or a pathologist reads a specimen but never sees the patient. Since the Radiologist and the Pathologist are participating in the treatment of the patient, providing indirect services, the Radiologist and the Pathologist are not considered Business Associates of the medical practice.***

A Covered Entity may also be a Business Associate in some cases. For example, a hospital that provides billing services to a medical practice is considered to be a Business Associate.

In this example, the medical practice needs to execute a Business Associate Agreement with the hospital for the provision of those billing services.

Marketing and Fundraising

For most activities and communications that are considered "marketing" under the Privacy Rule, the practice must obtain the patient's authorization to use or disclose their PHI.

WHAT IS MARKETING?

"To make a communication about a product or service, that encourages recipients of the communication to purchase or use the product or service."

Part II, 45 CFR 164.501

The activities listed below are not defined as marketing activities and therefore **do not** need an authorization:

◆ The use of a patient's PHI to further that patient's particular treatment. For example, a physician's recommendation of a specific name brand pharmaceutical or over-the-counter pharmaceutical or a referral of that patient to another provider is not considered "marketing" under the Privacy Rule.

◆ The use of a patient's PHI in the course of managing or coordinating that individual's treatment or recommending alternative treatment, therapy, providers or settings. For example, reminder notices for appointment, annual exams or prescription refills are not marketing.

◆ The use of a patient's PHI in describing if and whether a product or service or payment for the same is covered by the patient's benefit plan or otherwise payable by a Covered Entity is not marketing.

Even though the Privacy Rule generally requires a patient's authorization prior to using the patient's PHI for marketing purposes, the following marketing activities within or by a practice **do not require an authorization**:

◆ A marketing communication that is face-to-face with the patient. For example, if the provider is providing sample products to the patient during an office visit.

◆ A marketing communication that involves the provision of products or services of nominal value, such as pens or toothbrushes with the practice name on it.

However, should the practice receive "financial remuneration" in exchange for making the marketing communication, an authorization would be required. "Financial remuneration" means the direct or indirect payment from or on behalf of a third party whose product or service is being described, but does not include any payment for treatment of a patient.

To further clarify marketing, the activities listed below are examples of marketing activities that require a patient's authorization:

- Selling or giving away lists of patients.

- Receiving payment from a vendor for marketing a particular product to your practice's patients. For example, a dermatologist receiving payment from a sunscreen manufacturer for recommending a particular sunscreen to his/her patients.

- Asking patients to invest in such things as multi-level marketing schemes or in a building such as a new medical office building.

- Selling or giving away a list of patients to a Business Associate or other vendor. In this case, authorization must be obtained from each patient on the list.

With respect to fundraising communications, i.e, when a practice uses or discloses certain types of information of a patient for purposes of raising funds for its own benefit, in each such communication, the practice must provide a clear and conspicuous opportunity for the patient to opt-out of receiving future fundraising communications. The practice is free to determine the method by which a patient may opt-out, as long as it does not cause undue burden to the patient. While a written statement would be best, if an oral statement is given, such an oral opting-out should be documented in the patient's file.

The practice cannot condition treatment or payment on an individual's choice to receive or not to receive fundraising communications, and once a patient has decided to opt-out, the practice may not send fundraising communications to him. However, the practice may provide a patient who has opted-out with a chance to opt back in.

Personal Representatives Under HIPAA

Generally

Under HIPAA, a "personal representative" is treated as if he or she is the individual who is the subject of the PHI.

WHAT IS A PERSONAL REPRESENTATIVE?

A person is a "personal representative" of a living individual if, under applicable law, the person has the authority to act on behalf of an individual in making decisions related to healthcare (e.g., guardians, persons with power of attorney, etc.).

"Decisions related to healthcare," according to the Privacy Rule refers to making treatment and payment decisions on behalf of the patient. The Privacy Rule provides the following illustrative example: a husband may have the authority to make decisions about his wife's healthcare in an emergency; however, he may not have the right to access PHI related to treatment she received ten years ago.

The rule differs somewhat for decedents. A person may be a personal representative of a deceased person if he or she has the authority to act on behalf of that individual or the individual's estate for any decision, not just those decisions related to healthcare (such as an executor of the estate). The difference lies in the fact that the decedent cannot authorize that PHI be **disclosed**, whereas a living individual may do so.

The Special Case of Minors

Your practice may have to determine whether a person has the authority to act as the personal representative of a minor. Unfortunately, the Privacy Rule is not very clear regarding preemption of state laws concerning minors. While most state laws are preempted by HIPAA if the law is less protective of the privacy of the patient, the Privacy Rule treats minors differently. ***HIPAA defers to all state laws regarding the disclosure of minors' health information to a parent, whether that law provides greater or lesser protection to the individual.***

An analysis of your state law is necessary in order for the practice to determine how to handle the PHI of minors. The practice should answer the following questions:

Question 1:

Has the minor been abandoned by his/her parents or guardian and considered "emancipated" under state law?

The qualifications for an emancipated minor vary from state to state. Generally, the minor must be of a certain age (for example, 16 or 18 years old) and have established some level of independence from

his/her parents or guardians. If the minor is emancipated, and the minor has not established anyone as his/her personal representative, then the practice should deal only with the minor with issues concerning his/her PHI.

Question 2:

If the minor is not emancipated, does he/she have the authority to control his/her health information?

Under HIPAA, there are three circumstances in which a minor who is not emancipated has the authority to control his/her health information.

◆ If the minor signed a consent for the health care services that is valid for the provision of such services under state law, no other consent is needed by anyone regardless of whether or not the person is a personal representative of the minor. This ***requires*** a review of state law. It is important to note the distinction between the control of the health information (generally addressed by HIPAA) and the provision of health care services to minors (generally addressed by state law). If the minor can consent to the receipt of health care services under state law, HIPAA permits the minor to also control the resulting health care information.

◆ The minor legally can obtain health care services without the consent of a parent or guardian, as long as the minor, a court, or another person authorized by law has consented to the health care services. This **requires** a review of state law.

◆ A parent or guardian has agreed to confidentiality between a provider and the minor with respect to the healthcare service.

Practices should pay particular attention to any state laws concerning mental health, substance abuse, birth control, or sexually transmitted diseases, which frequently address minors. State laws may create greater rights of privacy and control for minors, or may result in greater disclosure rights for parents and guardians.

Question 3:

If the minor is not emancipated, and does not qualify for one of the exceptions described under Question 2, does the parent or guardian have the authority to act as a personal representative of the minor?

Your practice should treat a person as a personal representative of the minor with respect to his/her PHI if: (1) none of the criteria set forth in Question 2 are met, and (2) ***by state law*** the parent or guardian has the authority to act on behalf of the minor in making healthcare decisions.

Enforcement and Penalties Under HIPAA

The U.S. Department of Health and Human Services' Office of Civil Rights (OCR), has been assigned the authority to enforce the Privacy Rule. The OCR has several responsibilities:

1. Investigating complaints it receives from individuals who believe that a covered entity such as a medical practice is not complying with HIPAA's privacy requirements;

2. Providing covered entities such as a medical practice with assistance in order to achieve compliance; and

3. Making determinations regarding exceptions to state law pre-emption. Any person or organization can file a complaint with the OCR, but complaints typically must be filed within 180 days of the occurrence of an action in violation of the Privacy Rule.

Your practice is required to maintain records related to its compliance with the Privacy Rule in order for OCR to determine whether it is in compliance with HIPAA's requirements. Additionally, your practice must cooperate with an OCR investigation or compliance review should these occur.

Improper use or disclosure of PHI can result in the following fines and/or imprisonment, as set forth under HIPAA:

- Civil monetary penalties for HIPAA privacy violations are as follows:

Conduct which gives rise to violation	Penalty
Practice did not know (and by exercising reasonable diligence would not have known) of a HIPAA violation	$100 to $50,000 per violation; Up to $1,500,000 total per calendar year for repeated identical violations
HIPAA violation is due to reasonable cause and not due to willful neglect	$1,000 to $50,000 per violation; Up to $1,500,000 total per calendar year for repeated identical violations
HIPAA violation is due to willful neglect but the violation is corrected within the required time period	$10,000 to $50,000 per violation; Up to $1,500,000 total per calendar year for repeated identical violations
HIPAA violation is due to willful neglect and is not corrected	Fine of not less than $50,000 per violation; Up to $1,500,000 total per calendar year for repeated identical violations

◆ A person who knowingly violates HIPAA and obtains IIHI or discloses IIHI to another person may be fined up to $50,000 and imprisoned up to one year, or both.

◆ If the offense is committed under false pretenses, the fine may be up to $100,000 and imprisonment up to five years.

◆ If the offense is committed with the intent to sell, transfer, or use IIHI for commercial advantage, personal gain, or malicious harm, the fine may be up to $250,000 and imprisonment up to 10 years.

The Relationship Between HIPAA and State Privacy Laws

PLEASE NOTE:

THIS MANUAL DOES NOT INCLUDE A REVIEW OF STATE LAWS OR REGULATIONS THAT MAY CONTINUE TO APPLY AFTER THE PUBLICATION OF THE HIPAA REGULATIONS. ***You should consult with advisors familiar with your state's laws to determine which laws and regulations will impact the operation of your practice. Alternatively, consult with your state medical society or chapter of your specialty society.***

Most states have privacy laws already in existence. It is a huge task to determine how the state's privacy requirements compare to the federal HIPAA requirements. For example, Virginia has over 90 privacy laws. Thus, you can see why it is important that each practice consult with either their state or local chapter of their medical society as well as with an attorney who is familiar with your state's laws as they relate to privacy.

You should think of HIPAA as a federal privacy "floor," since the regulations represent a national set of minimum standards. Generally speaking, a federal privacy "floor" means that if a state's laws are not as stringent as HIPAA, then the federal privacy regulations will apply. In the event that a state's laws are more stringent or provide greater privacy rights or protections to patients, then the state's law (in most instances) will continue to apply. In other words, only in limited instances will HIPAA "pre-empt" state law. For example, state law is pre-empted if HIPAA's requirements are "contrary" to state law (that is, your practice cannot comply with both the state and federal standards, or the state law is "an obstacle to the accomplishment and execution" of the full purposes and objectives of HIPAA).

Examples of the types of state laws that will continue to apply:

◆ State laws concerning a compelling public health, safety, or welfare need, or regulation of controlled substances. For example, if your state requires that your practice report incidents of certain infectious or contagious diseases to state authorities (e.g., tuberculosis), these laws will continue to apply.

◆ State laws that are more stringent, such as those laws that prohibit a particular use or disclosure of patient information that would be permitted under HIPAA, for example statutes and regulations related to HIV status, mental health and substance abuse. More stringent laws also include those statutes and regulations that permit individuals greater rights to their information. Common examples of these types of laws include statutes and regulations related to access or amendment. For instance, HIPAA requires that patients be provided with access to their PHI within 30 days of a request (with certain exceptions); however, some states require that access be granted more quickly.

◆ State laws regarding the disclosure of minors' health information to a parent, whether that law provides greater or lesser protection to the individual.

Again, we must remind and urge you to check with your state or local medical association, attorney or specialty association to determine what type of information they may have on your state's privacy regulations.

Step 2: Select a Privacy Officer

The practice must designate a Privacy Officer or generally, a responsible person in the practice (who we will refer to as the "Privacy Officer") who will be responsible for the implementation and oversight of the Privacy Rule as well as for the development of the practice's policies and procedures regarding the Rule. This position will be responsible for implementing whatever changes or modifications need to be implemented as identified during your risk assessment and as required by the Privacy Rule.

In smaller practices, the office manager or other designated individual will typically assume these duties within his/her current job. For larger practices (20 or more physicians), it may be necessary to designate a full-time additional employee as the Privacy Officer. It is the responsibility of the individual practice to determine whether or not it should designate someone full-time for this position.

IDENTIFY YOUR PRIVACY OFFICER:

Name of Privacy Officer: _____

Practice Name:_____

Date:_____

• The HIPAA Privacy Rule ***does not*** require that ***an additional*** employee be hired to perform these duties. The HIPAA Privacy Rule mandates that ***someone*** within the practice ***must be responsible*** for carrying out these duties. It is up to the practice to determine whether or not they need to hire someone specifically to be the Privacy Officer or to have a current employee absorb the duties into his/her job description.

• Practices may consider sharing a Privacy Officer or outsourcing these responsibilities to an outside entity, such as a consultant or attorney. For example, one person may be the Privacy Officer for more than one practice. Each practice should determine how it can best delegate the Privacy Officer responsibilities.

Step 3: Review and Implement Privacy Officer Responsibilities

See Exhibit 1 for the Privacy Officer Job Responsibilities.

To do:

- Fill in your Practice Name on Exhibit 1.
- Document when Privacy Officer responsibilities are adopted and/or revised.
- Privacy Officer responsibilities were:

Adopted:_____
Date

Revised:_____
Date

Revised:_____
Date

- As additional clarification of the Privacy Rule is provided by HHS, these responsibilities may be modified.
- Place this form and other relevant forms in a permanent HIPAA Privacy folder or binder to serve as part of your practice's overall Compliance Plan.

Step 4: Conduct a Walk-Through of the Practice to Identify Privacy Risk Areas

See Exhibit 2 for Your Internal Privacy Checklist.

In order to determine how compliant your practice is with the Privacy Rule, your practice must examine its facility layout and practice operations as these relate to privacy.

The standard for minimum necessary use requires that physician practices make a reasonable effort to limit access to PHI only to those employees who need it based on their job descriptions. Because of this it is important that PHI is not visible where unauthorized individuals (employees or outsiders) might see it. All practices should make a concerted effort to accomplish this. However, it is recognized that some practice staff must all have access to all PHI in order to carry out their job responsibilities.

In order to assess your practice's risk areas related to privacy, the Privacy Officer should begin at the front door of your practice and utilize the Internal Privacy Checklist provided in Exhibit 2 as a guide to auditing each area of the practice. The objective is to identify areas where unauthorized individuals potentially have access to patients' PHI and/or where the minimum necessary standard might be negatively impacted.

To do:

• Fill in your Practice Name on Exhibit 2.

• Photocopy Exhibit 2 (all pages) for the facility in which your practice operates. If you have more than one facility, photocopy Exhibit 2 (all pages) for each facility.

• Follow the checklist through all areas of your practice including the front office, clinical areas, medical records, and business office areas.

• Answer the questions to identify what your current operational procedures are for these areas. Note: Many functions and operations are repeated. This is to make certain that you don't miss any areas of operation.

• Make reasonable modifications to incorporate the suggested guidelines for policy adherence into your practice facility and operations.

Note:

• If multiple locations are operated by your practice, this walk through must be conducted at each location.

continued

• Medical practices are NOT required by the Privacy Rule to completely restructure their facilities and office space since the HHS does not consider restructuring and redesigning facilities necessary. However, some moderate redesign to your practice's existing layout and design, as well as to your method of conducting business, may be appropriate or desirable in order to minimize access to PHI.

Step 5: Implement a Notice of Privacy Practices

See Exhibit 3 for Your Notice of Privacy Practices.

Your practice must implement and maintain an official Notice of Privacy Practices to inform patients about their rights surrounding the protection of their PHI. This notice must be displayed in an area of the office where patients will readily see it, such as in the waiting room or reception area and must be given to patients the first time services are rendered.

This notice is long due to the complexity required by the regulation itself. A written summary alone would not be acceptable because it would require the omission of language that protects your practice.

Patient Rights

Under HIPAA, an individual has the following rights with regard to his/her PHI:

- The right to authorize the use and disclosure of PHI for certain non-TPO purposes and for psychotherapy notes.
- The right to receive a copy of the practice's Notice of Privacy Practices.
- The right to request restrictions on certain uses and disclosures of PHI.
- The right to request restrictions on how the practice communicates PHI to the patient.
- The right to inspect and copy PHI.
- The right to request an amendment of PHI.
- The right to an accounting of the disclosures of PHI made by the covered entity for purposes other than TPO and not pursuant to a valid authorization.
- The right to complain about alleged violations to the practice and DHHS.

To do:

• Fill in Practice Name on Exhibit 3.

• Photocopy and distribute the Notice of Privacy Practices to patients on the day services are first rendered. If you offer a patient the opportunity to receive a copy of the Notice of Privacy Practices via e-mail and the patient accepts, you may distribute a copy of the Notice via e-mail to an e-mail address that they provide. However, if you receive confirmation that your attempt to provide the Notice of Privacy Practices via e-mail has failed, you must deliver a paper copy of the Notice of Privacy Practices to the requesting individual.

• Use best efforts to obtain written acknowledgement from the patient that he/she has received a copy of the Notice of Privacy Practices. If you are unable to obtain such authorization, your efforts must be documented in the chart notes and a reason given for not obtaining the acknowledgement.

• Post the Notice of Privacy Practices in an area in your practice where it is clearly visible to patients. If it is revised, the revised version must be distributed to each patient upon his or her request and posted prominently in the practice.

• If your practice has a web site that describes its services and benefits, a copy of the Notice of Privacy Practices must be posted on the web site.

• Create an electronic copy of Notice of Privacy Practices in a "read only" version that can only be modified by the Privacy Officer.

Notes:

• Some clauses have been defined in the Privacy Rule as "Optional." Include the "Optional" clauses only if they are applicable to your practice.

• You must provide your Notice of Privacy Practices to all patients no later than the first delivery of service. Non-patients also have the right to obtain a copy.

• If you want to put more stringent restrictions than legally required on how you use and disclose PHI, you may do so, according to the HIPAA Privacy Rule. However, the restrictions cannot infringe upon the uses and disclosures that are required by the Privacy Rule.

• If you are applying greater limits on uses and disclosures of PHI than previously stated, a statement acknowledging this change must be included in a revised Notice of Privacy Practices.

• Although you are permitted to revise your Notice of Privacy Practices (so long as it continues to comply with the Privacy Rule), you must reserve this right in writing in your Notice of Privacy Practices. ***The Notice of Privacy Practices provided to you in this Manual reserves this right to you — be sure not to remove it.***

• Whenever there is a change that needs to be made to the Notice of Privacy Practices such as to the uses and disclosures of PHI, to the individual patient's rights or to the practice's legal duties, the practice

must revise and have available for redistribution the Notice of Privacy Practices to its patients in a timely manner. There is no requirement to mail or otherwise send the revised notice to patients.

• You must retain a complete copy of each version of the Notice of Privacy Practices for six years. Accordingly, if a Notice of Privacy Practices is superseded by a new version, you only need to keep the old version for six years.

• If you maintain a web site that provides information to patients, you must post the Notice of Privacy Practices on your web site. The Notice of Privacy Practices can also be provided by e-mail. However, the patient must agree before this notice can be sent electronically.

Step 6: Implement a Written Acknowledgement Process

See Exhibit 4 for the Receipt of Notice of Privacy Practices Written Acknowledgement Form.

You must distribute the Notice of Privacy Practices to all patients the first time services are rendered. In addition, you must use best efforts to obtain written acknowledgement from the patient that he/she has received a copy of it.

To do:

• Fill in Practice Name in Exhibit 4.

• Use best efforts to obtain written acknowledgement from the patient that he/she has received a copy of the Notice of Privacy Practices.

Notes:

• If you are unable to obtain such authorization, your efforts must be documented in the chart notes and a reason given for not obtaining the acknowledgement.

• If a practice fails to obtain written acknowledgement from the patient of receipt of the Notice of Privacy Practices, then the practice must document its efforts to obtain the written acknowledgement and the reason why the written acknowledgement was not obtained (e.g., a patient refused to sign).

Step 7: Implement Privacy Policies and Procedures

See Exhibit 5 for Your Sample Privacy Policies and Procedures

The practice must develop and implement policies and procedures with respect to PHI that are designed to comply with the Privacy Rule. Although the policies and procedures must be reasonably designed, taking into account the number and type of activities that relate to PHI undertaken by the practice, this requirement is not to be construed to permit or excuse an action that violates the Privacy Rule.

Your practice's Notice of Privacy Practices (See Exhibit 3) informs patients about their rights surrounding the protection of their PHI. From this, a practice must develop privacy policies and procedures in order to be compliant with the patients' rights described in the Notice of Privacy Practices. Sample Privacy Policies can be found in Exhibit 5. For those practices unfamiliar with how to develop practice procedures from policy, a sample Privacy Procedure can be found in Exhibit 5.

To Do:

- Fill in Practice Name in Exhibit 5.
- Take the sample Privacy Policies and develop corresponding procedures to accomplish the policy statements.
- Incorporate the Privacy Policies and Procedures into all appropriate documents, including your practice's Personnel Policies and Procedures Manual, Employee Handbook and/or Compliance Plan.

Notes:

- Privacy Policies and Procedures must be retained for six years from the date of creation or the date when it was last in effect, whichever is later.
- Retain these Privacy Policies and Procedures in your HIPAA Privacy Rule folder or binder.

Step 8: Implement a Patient Authorization Form

See Exhibit 6 for the Patient Authorization Form.

See Exhibit 7 for Illustrations of Situations Requiring/Not Requiring Authorization.

An authorization is *required* for use and disclosure of PHI for most non-TPO purposes. An authorization has an expiration date, and states the purpose for which the information may be used or disclosed.

Exhibit 7 will assist your practice in determining when an Authorization Form is needed and when it is not.

To do:

• Fill in Practice Name on Exhibits 6 and 7.

• Photocopy and make available the Patient Authorization Form at each facility in which your practice operates.

• Notice of Privacy Practices will inform patients that most non-TPO uses and disclosures will require patient authorization.

• Determine if situations in your practice will require authorization for disclosure of PHI. ***See Exhibit 7*** for the list of situations.

Notes:

• When these situations occur, the staff must inform the patient of the authorization requirement and request that the patient sign an Authorization Form.

• If the patient refuses to sign the Authorization Form, then the practice cannot use or disclose the PHI for purposes outside of TPO.

• Original Form is retained in the patient's medical record.

• Once the document is signed, the practice is required to provide a copy of the signed authorization to the patient. In addition, the practice must retain a record of the authorization for six (6) years at a minimum.

continued

• All providers, not just direct treatment providers, must obtain an authorization to use or disclose PHI for purposes other than TPO. (A direct treatment relationship is when a healthcare provider provides direct care to an individual. When the care is delivered through another healthcare provider, it is NOT a direct treatment relationship, but an indirect treatment relationship. An example of a direct treatment relationship is a provider who treats a patient in person in his/her office. An example of an indirect treatment relationship is a radiologist who reads an x-ray for another provider. In this example, the radiologist possibly never sees the patient in person).

• Treatment of patient ***cannot*** be conditioned based on completion of authorization. The only exception to this is when the treatment is related to research and for treatment that is solely for the purpose of creating PHI for disclosure.

• If the practice will receive any payment from a third party for using and disclosing the patient's PHI, then it needs to state so on the patient Authorization Form.

Step 9: Implement a Form Requesting Restrictions on Uses and Disclosures of PHI

See Exhibit 8 for the Request for Limitations and Restrictions of Protected Health Information Form.

According to the Privacy Rule, a practice is required to accommodate reasonable requests by patients to restrict how their PHI is used and disclosed. If the practice is unable to accommodate a request, then the practice needs to document and inform the patient of its denial. The restriction is not applicable if such information is needed to provide emergency treatment.

The practice may terminate its agreement to a restriction if:

- The individual agrees to the termination in writing;
- The individual orally agrees to the termination and the oral agreement is documented; or
- The covered entity informs the individual in writing that it is terminating its agreement to the restriction.

See Exhibit 8 for the form for patients to complete when they want to request a restriction on the uses and disclosures of their PHI.

To Do:

• Fill in Practice Name on Exhibit 8.

• Photocopy and make available copies of the forms at each facility in which your practice operates to distribute to patients **upon their request**.

• If patient requests restrictions on PHI, provide them a form and explain to them how to complete it.

• Privacy Officer should review request and make arrangements to accommodate reasonable requests.

• Privacy officer should contact patients and discuss unreasonable requests.

• The Notice of Privacy Practices will make patients aware of this opportunity. It is not necessary to inform them individually.

continued

• The form should be completed in person while patient is in the office. If the form is sent to the practice, the practice should make certain that the patient's signature matches the signature on file.

• The form should be submitted to the Privacy Officer.

Notes:

• A practice that agrees to a restriction must document the restriction and maintain a record of it for six (6) years according to the HIPAA requirements. Please review your state's laws concerning retention of medical records to see if any stricter standards apply.

• The practice must permit patients to request and must accommodate reasonable requests to receive communications of PHI from the practice by alternative means (for example, by mail rather than telephone) or at alternative locations (for example, at home rather than at work). The practice can require that this request be submitted in writing. The practice cannot require the patient to provide an explanation for the request.

• The practice must grant a patient's request for a restriction in disclosures of PHI if the disclosure is for payment or health care operations and if the PHI pertains to a service for which the patient paid in full, out of pocket. Bear in mind that no restriction on disclosure applies when the disclosure is made for treatment purposes.

• The patient is **NOT** required to use the form provided in Exhibit 8. This form is provided as an example of what a practice can choose to use, although the Privacy Rule does not require it. If the patient chooses, he/she may handwrite their request on any piece of paper.

Step 9A: Receipt of Requests for Confidential Communications of PHI

Communications of PHI

The Privacy Standards state that a covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications containing PHI by alternative means or at alternative locations. For example, an individual who does not want his family to know about a certain treatment may request that the provider communicate with the individual about that treatment at the individual's place of employment, by mail to a designated address, or by phone to a designated phone number. Covered health care providers must accommodate all reasonable requests.

The reasonableness of a request must be determined by a covered entity solely on the basis of the administrative difficulty of complying with the request (e.g., if a patient only works the 11pm – 7am shift and wants to be contacted by telephone at work, this would be viewed as unreasonable). A covered health care provider cannot refuse to accommodate a request based on its perception of the merits of the individual's reason for making the request, nor may the health care provider require the individual to provide a reason for the request. A health care provider may refuse to accommodate a request, but only when the individual has not provided information as to how payment, if applicable, will be handled, or when the individual has not specified an alternative address or method of contact. Additionally, a covered entity may require an individual to submit requests for confidential communications in writing.

Notes:

• The Notice of Privacy Practices will make patients aware of this opportunity. It is not necessary to inform them individually.

• The practice may require that this request be submitted in writing. The practice may not require the patient to provide an explanation for the request.

• If the request is sent to the practice, the practice should make certain that the patient's signature matches the signature on file.

• The request for confidential communications should be submitted to the Privacy Officer.

• A practice that agrees to a type of confidential communication must document the restriction and maintain a record of it for six (6) years according to the HIPAA requirements. Please review your state's laws concerning retention of medical records to see if any stricter standards apply.

Step 10: Implement a Form to Inspect and Copy PHI

See Exhibit 9 for the Request to Inspect and Copy Protected Health Information Form.

According to the Privacy Rule, patients have the right to request to inspect and copy their PHI. This is provided as a general guideline in Exhibit 9. However, the practice is not required to agree to such a request. Please see Step 11 and Exhibit 10 for the reasons that a practice can deny a patient access to their PHI. In cases where the patient is a minor acting as his/her own personal representative, whose custody may be in dispute, or who may be in an abusive situation, **practices should refer to their state law for guidance about parental access.**

To Do:

• Fill in Practice Name on Exhibit 9.

• Photocopy and make available the form for patients to inspect and copy their PHI as requested under the Notice of Privacy Practices.

• Although it is preferred that the form be completed by the patient in person while the patient is present in the office, this is not required. If the form is sent to the practice, you should make your best effort to determine that the patient's signature matches his/her signature on file. The patient cannot be required to use the practice's form, although the patient may be required to submit the request in writing.

• The form should be submitted to the Privacy Officer.

Notes:

• The practice must inform patients that a written request is necessary.

• You may charge the patient a reasonable rate for copying their record. Charges should be based upon the actual cost of supplies, labor, postage and copying. Please note that state law may limit copy charges.

• If a patient wishes to inspect his/her record, he/she should do so in a private area provided by the practice overseen by the Privacy Officer or his/her designee present.

• The practice must respond to requests within 30 days for information stored onsite and within 60 days for information stored offsite. The practice can request one 30-day extension, if it provides the patient with a written notice of the reason for the delay.

continued

• The information must be provided to the patient in the form or format requested by the patient if readily producible, including electronic formats if so requested by the patient.

• If access is denied, the patient must be notified in writing in a timely manner, and the notification must explain the basis for the denial. See Exhibit 10. If the grounds for denial are reviewable, the practice must describe the patient's review/appeal rights in the written notice.

Step 11: Implement Access Denial Form

See Exhibit 10 for the Patient Denial Letter.

Although patients have the right to request to inspect and copy their PHI, practices are not required to agree to their request. Under the Privacy Rule, practices have the right to deny requests for PHI under the following circumstances:

- Requests for psychotherapy notes (See glossary for definition.)
- Requests for PHI that is being used in a civil, criminal or administrative action or proceeding.
- Requests for PHI that is subject to or exempted from the Clinical Laboratory Improvements Amendments (CLIA) of 1988. CLIA states that clinical laboratories may provide clinical laboratory test records and reports only to "authorized persons" as defined primarily by state law. In some cases, the patient is not always included in the group of authorized persons. HIPAA does not preempt CLIA and therefore, covered entities that are subject to CLIA are not required to provide a patient access to their PHI if CLIA prohibits them from doing so. If your medical practice is not subject to CLIA, then this denial reason does not apply and should be disregarded.
- Requests for PHI that was obtained from someone other than a healthcare provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
- Requests for PHI that was/is being created or obtained in the course of ongoing research where the patient agreed to the denial of access when he/she consented to participate in the research.
- Requests for PHI that is contained in records subject to the federal Privacy Act. This Act protects personal information about individuals held by the federal government. Covered entities that are federal agencies or federal contractors that maintain records that are covered by the Privacy Act not only must comply with the Privacy Rule's requirements but also must comply with the Privacy Act.
- Requests for PHI that the healthcare professional has determined in his/her professional judgment that access to the PHI is reasonably likely to endanger the patient's life or physical safety or the life or physical safety of another person.
- Requests for PHI that makes reference to another person and that a licensed healthcare professional has determined is reasonably likely to cause substantial harm to such person(s).

◆ Requests for PHI where the request is made by the personal representative of the patient (who is the subject of the information) and a licensed healthcare professional, decides according to his/her professional judgment, that the PHI should not be provided.

If a practice denies requests for any of the last three reasons, then the patient has the right to submit a written request to the Privacy Officer to have the denial reviewed by another licensed healthcare professional who did not participate in the original denial. The Privacy Officer must respond with a written decision within a reasonable period of time. The patient can also file a complaint with the Secretary of the HHS.

There may be circumstances where the practice may partially agree or disagree with a patient's request. In this case, the same procedures will apply. The request must be reviewed and a written decision must be given to the patient that describes what the practice agrees to and what it does not. Again, the patient can file a complaint with the Secretary of the HHS if he/she is not satisfied.

To do:

• Fill in Practice Name on Exhibit 10.

• Photocopy and complete the Patient Denial Letter as necessary to respond to requests.

Step 12: Implement a Form to Amend PHI

See Exhibit 11 for the Request for Correction/Amendment of Protected Health Information Form.

According to the Privacy Rule, patients have the right to request to amend their PHI. This may occur when a patient feels that his/her PHI is inaccurate or incomplete. Providers should review the patient's amendment request and decide whether or not it is appropriate to agree with the request.

It is important to always use the correct procedure if the physician agrees to amend a medical record. A single line should be drawn through the erroneous entry. The correct entry should be placed after the last entry, the change explained, and the change dated and initialed. Do not scratch out or "white-out" an error. Never attempt to supplement, complete, clarify, or amend a medical record after being notified of a legal claim involving the record or the care of the patient.

To do:

• Fill in Practice Name on Exhibit 11.

• Photocopy Exhibit 11 and make available the form for patients to amend their PHI.

Notes:

• Notice of Privacy Practices will make the patient aware of this opportunity.

• Although it is preferred that the form be completed by the patient while he/she is present in the office, this is not required. If the form is sent to the practice, you should make your best effort to determine that the patient's signature matches his/her signature on file. The patient cannot be required to use the practice's form, although the patient may be required to submit the request in writing.

• The form should be submitted to the Privacy Officer.

• The Privacy Officer should submit all forms to the appropriate provider for review.

• The patient's provider should review his/her patient's request to amend their PHI and decide whether or not the request is valid.

• The provider should submit his/her response in writing to the patient. If the request is denied, the response should include an explanation for the denial.

continued

• If applicable, the provider or a designated staff member should document the amendment in the patient's medical record, and should record the date, the amended PHI and the initials of the person who recorded the amendment.

• A provider is not required by the Privacy Rule to agree to the amendment of PHI.

• The practice must respond within 60 days of the request. The practice can request one 30-day extension if it provides the patient with written notice of the reasons for the delay.

• Records of requests to amend PHI must be maintained for six (6) years.

• Future disclosures of the patient's PHI must include the individual's request for the amendment, the amended PHI (if applicable), or a copy of the provider's denial letter (if applicable).

Step 13: Implement a Form to Request an Accounting of Disclosures of PHI

See Exhibit 12 for the Request for an Accounting of Protected Health Information

According to the Privacy Rule, patients have the right to request an accounting of some disclosures of their PHI. However, the practice does not have to account for disclosures made: directly to the patient; for certain other purposes such as national security or to correctional institutions; for disclosures made pursuant to an authorization; for incidental disclosures; and for disclosures that are part of a Limited Data Set (when such Limited Data Set is disclosed pursuant to a Data Use Agreement).

If the practice is required to account for a disclosure (discussed further below), the practice must keep a record of the disclosure, for the patient. The disclosure record for each patient must indicate to whom their PHI was disclosed, what information was disclosed, and the date it was disclosed.

The medium through which the disclosure is made is very important.

For purposes of HIPAA, a disclosure can be made "through" an electronic health records (EHR) system, or not.

Obviously, if the practice does not have an EHR system, it will not be disclosing anything "through" an EHR system.

If the practice has an EHR system, then an example of a disclosure "through" an EHR would be transmission of a prescription from the practice to a pharmacy ("treatment"), via the EHR. The use of the EHR to make the disclosure is important because the software can be designed to track the disclosure automatically, without human involvement. This makes it much easier to track routine or frequent disclosures, such as TPO disclosures.

If the disclosure is made "through" the EHR system, then the disclosures which must be tracked and accounted for include both TPO and non-TPO disclosures. Check with your software vendor to make sure that your software has the capability to track these disclosures automatically, and then print out a report upon request.

If the disclosure is not made through an EHR, then the practice is only required to track disclosures of non-TPO. There is no obligation to account for TPO disclosures made in this fashion.

Thus, a practice without EHR would need to track and account for a patient chart which is mailed to an attorney in response to a subpoena (disclosure was made for non-TPO purposes.) But if the patient's PHI were mailed to another medical practice, such as referral to a specialist for treatment, then there

would be no obligation to account for the disclosure, because it is a TPO disclosure not made through an EHR.

The time period for which the accounting is required also depends on the medium through which the disclosure is made.

If the disclosure is not being made through an EHR system, then the practices is only required to give an accounting for the six (6) years preceding the date of the request.

If the disclosure is being made through an EHR, the required accounting period is only three (3) years preceding the date of the request.

Note the effective dates for the special EHR disclosure requirements outlined above.

The effective date of the EHR accounting requirement for entities that acquired an EHR after January 1, 2009 is January 1, 2011, or the date the practice acquired the EHR, whichever is later.

For practices that acquired an EHR prior to January 1, 2009, the effective date of the EHR accounting requirement is January 1, 2014.

The following chart summarizes the requirements:

Disclosure Medium	**TPO Included?**	**Limit on Length of Look back**
Through EHR	Yes; must account for all disclosures, including TPO	3 years prior to date of request
Other than through EHR	No; TPO disclosures do not have to be accounted for when the disclosure is made outside the EHR. Only non-TPO disclosures must be accounted for.	6 years prior to date of request

The format in which the PHI is provided to the patient is also important.

Patients have a right to obtain an electronic copy of their PHI regardless of whether the covered entity or business associate uses an EHR; put another way, patients are entitled to an electronic copy of their PHI, regardless of whether that PHI was historically maintained by the practice in paper form or in electronic form.

Additionally, if the patient requests an electronic copy of PHI that is maintained by the practice in electronic form, the practice must provide the individual with access to the electronic information in the electronic form and format requested by the patient, if it is readily producible, or, if not, in a readable electronic form as agreed to by the practice and the patient. The practice must provide the patient with the information requested in a designated record set.

To do:

• Fill in Practice Name on Exhibit 12.

• Photocopy and make available the form to request an accounting of all disclosures of PHI.

• Maintain a list of all non-TPO disclosures going back 6 years. (An example would be a disclosure to a public health agency.) Ensure that your EHR system can track and report on all disclosures made through it, including TPO disclosures, for a period going back 3 years.

• The Privacy Officer enters information into (or assures that information is entered into) the Log to Track Disclosures of PHI (Exhibit 13) for disclosures made outside an EHR system, or ensures that another mechanism is used to track such disclosures of PHI.

• Provide Accounting of Disclosures of PHI to patient within 60 days of the request.

• Document the provision of the accounting to the patient and the title of the person/office receiving and processing the request and maintain the records for six (6) years.

• File original request form in patient's medical record.

Note:

• The extension for Accounting of Disclosures can be for no more than an additional 30 days and the practice is only allowed one (1) extension per request. Therefore, each accounting must be provided no more than 90 days after the request.

• The practice is required to provide the first accounting of disclosure request during any 12-month period free of charge. However, if a patient requests multiple accountings within a 12-month period, the practice can impose a reasonable, cost-based fee for each subsequent request, provided that the practice notifies the patient in advance of the fee.

• If the practice is unable to provide an accounting of disclosures within 60 days, the practice must provide the patient with written explanation of the delay and identify a date by which the practice will provide the patient with the accounting.

• The practice must temporarily suspend a patient's right to receive an accounting of disclosures to a health oversight agency or law enforcement official if such agency or official has provided the practice with a written statement saying that notifying the patient of this disclosure would conflict with the agency's or official's investigation. This written statement must include the time period for which the suspension is required.

Step 14: Implement a Log to Track Disclosures of PHI

See Exhibit 13 for a Log to Track Disclosures of Protected Health Information.

The practice must maintain a list of non-TPO disclosures that are not pursuant to an authorization, not merely incidental to another permitted disclosure, or that are part of a Limited Data Set (subject to a Data Use Agreement) for each patient. The practice is required to maintain such information for six (6) years (or three (3) years for disclosures made through the EHR).

If there have not been any non-TPO disclosures for a patient, and no disclosures were made through an EHR, then the practice is not required to keep a log for that patient.

However, disclosures of PHI made through an EHR system (whether TPO or non-TPO) must be accounted for. The look back period for these disclosures is the three (3) year prior to the patient's request.

If the practice has made multiple disclosures of PHI to the same person or entity for a single purpose or under a single authorization, the practice may with respect to such multiple disclosures provide:

- the date of the first disclosure during the accounting period;
- the name of the person/entity receiving the PHI;
- the name of the person/entity's address;
- a brief description of PHI disclosed;
- either the person/entity's authorization or a statement of the purpose of the disclosure;
- the frequency, time frame or number of disclosures made during the accounting period, and
- the date of the last disclosure during the accounting period.

To do:

• Fill in Practice Name on Exhibit 13.

• Photocopy the log to track disclosures of PHI.

Print out any required log of disclosures made through the EHR system.

• It is recommended that the patient's log be maintained on file in the patient's medical record or another secure place.

Step 15: Implement Patient Complaint Forms

See Exhibit 14 for the Suggested Patient Complaint Form.

The Privacy Officer is responsible for being the primary contact person for patients with questions, comments and complaints concerning privacy issues. Accordingly, the Privacy Officer should be designated to receive and respond to patient complaints pertaining to the practice's Privacy Policies and Procedures.

To do:

• Fill in Practice Name on Exhibit 14.

• Photocopy and make available the Patient Complaint Form upon request (optional; not required.)

• The Notice of Privacy Practices will inform patients of their right to request information or file complaints in regard to HIPAA and PHI.

• The Privacy Officer must document all complaints from patients and investigate them as appropriate.

• If the patient complaint is against a member of the practice's staff and this person is found to have not complied with the practice's Privacy Policies and Procedures, then the Privacy Rule requires that this person have appropriate sanctions or disciplinary actions applied against them.

• Revise your Personnel Policy and Procedures Manual to reflect disciplinary actions to employees who do not adhere to the Privacy Policies and Procedures.

Note:

• All patients and employees should be encouraged to communicate openly with the practice concerning any of their privacy concerns. No patient or employee may be intimidated, threatened, dismissed, coerced, or discriminated against for exercising his or her right to file a complaint with the practice or HHS. In addition, no patient can be asked to waive his/her privacy rights under the Privacy Rule.

• Patients are not required to use this form. This form was developed simply for the practice's benefit to make it easier for patients to communicate any issues they may have regarding the practice's Privacy Policies and Procedures. Patients may handwrite their complaint(s) on their own paper, in their own format, if they so choose.

Step 16: Determine Who Can Use and Disclose PHI

The **minimum necessary** standard states that a practice must identify those persons or job titles in the practice that must have access to PHI to carry out their duties. Once this is identified, the category or categories of PHI to which these persons need access must be identified. For example, certain employees will need access to patients' financial information while other employees may not. The purpose of this exercise is to limit the amount of use of PHI in the practice to only those individuals who need minimum necessary access to it to carry out their job responsibilities.

To do:

• Develop a list of staff that need to access PHI and determine which of those positions need which levels and kinds of access.

• Develop policies guiding staff as to the utilization of PHI based on job requirements.

• The Privacy Officer should maintain a master list of all employees, his/her authorized levels of access and his/her computer passwords.

• Develop appropriate restrictions to prevent unauthorized access to specific levels of PHI.

• Develop passwords (as necessary) restricting computer access to certain levels of information. Upon termination of employee, delete his/her password from system.

• Develop a policy outlining disciplinary actions to be taken for accessing PHI beyond an individual employee's minimum necessary need to know (security) level.

Note:

• All employees should review and be trained on policy requirements.

• The employee orientation checklist should be revised to include discussion of practice privacy policies regarding security of PHI and the expectations regarding their specific staff position.

• It may be necessary for all staff members of smaller practices to have access to all PHI in order to carry out their job responsibilities. Practices should make every effort to adhere to the minimum necessary standard by limiting the uses and disclosures of PHI within the practice. Common sense and practice need should be your guide.

Step 17: Update or Develop Job Descriptions with Respect to PHI Use and Disclosure

Job descriptions should be updated or, if not already in place, developed, for each staff member. These documents describe the responsibilities of each staff position and the level of access that he/she needs to PHI in order to perform the job. Job descriptions should be routinely reviewed for accuracy and appropriateness.

The practice policies and procedures governing access levels to PHI can be used as a guideline for developing or updating the job descriptions. These documents should address routine and/or recurring situations related to the minimum necessary standard.

For non-routine uses by staff, the practice must develop reasonable criteria for determining, and limiting use to, only the ***minimum*** amount of PHI ***necessary*** to accomplish the intended purpose. Non-routine uses and disclosures should be reviewed on a case-by-case basis so as to ask for only that information which is reasonably necessary for the purpose of the request. An example of a non-routine use would be if a nurse had to help the business office staff post patient receipts due to a staff shortage.

To do:

• Review current position descriptions and add minimum necessary standard PHI requirements.

• If job descriptions do not exist in your practice, you should develop them or, at the very least, develop separate written statements or documents outlining the minimum necessary PHI requirements for each position.

• Currently employed staff should be given copies of their revised job descriptions and sign a statement acknowledging that they have read and understand the revisions.

• The employee orientation should include a review of his/her current job description (inclusive of PHI security levels). Employee should sign a statement acknowledging that he/she has read and understood the job description.

Note:

• You must use your own judgment when deciding what the minimum necessary disclosure is of PHI to carry out TPO in your practice. The Privacy Rule is not meant to keep the practice from providing high quality patient care.

Step 18: Develop a List of Your Business Associates

See Exhibit 15 for a Listing of Typical Business Associates.

See Exhibit 16 for A Medical Practice Guide for the Privacy Officer to Identify Business Associates. (This exhibit need only be viewed by the Privacy Officer or Physicians.)

Most medical practices require the assistance of other businesses and contractors to carry out their day-to-day operational activities. These Business Associates, as they are referred to in the Privacy Rule, are any persons or entities that provide certain functions, activities or services for or to a medical practice involving the use and/or disclosure of PHI.

Note:

WHAT IS A BUSINESS ASSOCIATE?
A business associate is a person or entity that performs a function or activity on behalf of the practice involving the use and/or disclosure of PHI, but is NOT a part of the practice's workforce.

The determination of who is or is not a Business Associate can be somewhat vague, and is likely to vary from situation to situation. Let's consider several scenarios: A practice's janitorial service has no need to use or disclose your patients' PHI. The janitorial service would not be a Business Associate merely if they gained access to the practice's PHI. In fact, in the day-to-day routine of cleaning your facility, if PHI is routinely and openly visible, then you may have violated the Privacy Rule regarding failure to apply reasonable safeguards to protect patient privacy. However, if PHI is visible on only an incidental occasion, you have not violated the Privacy Rule. Incidental uses and disclosures that occur as a by-product of a use or disclosure that is otherwise permitted are not violations of the Privacy Rule. Another example could include legal services provided by a regulatory attorney to a medical practice. To the degree that such services do not include the disclosure of PHI, the attorney is not a Business Associate. However, legal services provided by a malpractice attorney will more likely involve the disclosure of PHI and therefore be more likely to characterize the malpractice attorney as a Business Associate of the medical practice.

Other variations involve indirect treatment providers. Another example could include treatment services provided by a radiologist or pathologist to a medical practice, in which the radiologist reads the patient's x-rays or the pathologist reads the slides for the medical practice, but never sees the patient face to

face. Since the radiologist and pathologist are participating in the treatment of the patient, they are not considered to be Business Associates of the medical practice.

With the proliferation of cloud computing and e-prescribing gateways, the determination as to who is a "Business Associate" gets more nuanced. For example, persons who provide data transmission services with respect to PHI and require access on a routine basis to PHI are Business Associates. While this area of HIPAA is still evolving, some things are clear. First, if an organization stores PHI, such as a cloud computing vendor, the cloud vendor or other organization would be considered to be a Business Associate. Second, "access on a routine basis" means more than a "mere conduit." So a person who provides courier services, such as the USPS or Federal Express, or a phone or internet provider who has random, occasional access to PHI, such as when it periodically reviews data transmitted over its network, would not be Business Associates under HIPAA. That being said, keep in mind that the "mere conduit" exception to the Business Associate definition is intended to be narrow and depends on the facts and circumstances of the service provider in question.

Subcontractors of a practice's Business Associate are considered to be Business Associates. They are required to enter into Business Associate Agreements with the practice's Business Associates (not with the practice).

In some situations, Covered Entities may be Business Associates of other Covered Entities. For example, a hospital may be contracted to provide billing services for a medical practice. In this example, the hospital is a Business Associate of the medical practice.

Exhibit 15 lists some "typical" Business Associates. Note that some of the persons or entities listed may NOT be Business Associates in your practice. This is why it is important for you to go through each step in Exhibit 16 to determine on a case-by-case basis if a person or entity is a Business Associate that you need to have sign a contract.

To do:

• Fill in Practice Name on Exhibits 15 and 16.

• Privacy Officer should compile a list of Business Associates.

• To accomplish this, review practice business files for contracts or other arrangements that are currently in place. One of the best ways to develop this list is to review your general ledger. This tells you to whom you have written checks and thus probably includes all or most of your Business Associates.

Contractors and vendors are not considered Business Associates if they do not have access to PHI. Keep in mind that pharmaceutical representatives, hospital staff and others that may have access to PHI (regardless of whether they receive money from the practice) may not need access to PHI to perform this function or activity and thus may not be properly characterized as Business Associates. To avoid

violating the Privacy Rule, these people should not be granted access to PHI. What may be considered a Business Associate in one practice may not be considered one in another. However, please note that those persons/entities who participate in the treatment of patients are not considered to be Business Associates of the medical practice.

• To determine if the person or entities are Business Associates, use the Flow Chart in Exhibit 16 for each person or entity.

Notes:

• Not all service providers may have a need to see PHI to perform this function or activity. The most common example is janitorial services, who do not require use or disclosure of PHI to perform their function or activity. These parties should not execute a Business Associate Contract and should not use or disclosure of PHI.

• The Business Associate list should be maintained on an ongoing basis. Each time your practice adds or discontinues a relationship with a party or entity, the list needs to be updated to reflect these changes.

• Similarly, each time the scope of services provided by a Business Associate changes, the relationship should be reexamined to confirm that the party continues to serve as a Business Associate.

• You should determine those persons or entities with current access to PHI that do not require such access for them to perform services on the practice's behalf. Anyone that is not a Business Associate (or a member of the practice's workforce) should not have access to PHI. Persons and entities that do not need PHI to perform services for the practice should not enter into Business Associate Agreements.

•Under HIPAA, Business Associates are now directly liable for compliance with the Privacy Rule, including its restrictions on use and disclosure of PHI, even if they have not signed a Business Associates Agreement. Nonetheless, medical practices are still obligated to sign appropriate Business Associate Agreements with all business associates.

• Some Business Associates may present you with their own version of a Business Associate Agreement. It is up to the practice to determine whether or not to use the contract in Exhibit 17 in this manual or the contract presented by the Business Associate. If you use the Business Associate's version of the contract, it is recommended that you compare it to the contract in this manual, or have a healthcare attorney or other knowledgeable person review it before executing the Business Associate Agreement.

Step 19: Implement Business Associate Agreements

See Exhibit 17 for a Model Form of Business Associate Agreement.

It is recommended that legal counsel review this model contract prior to use.

According to HHS, the Business Associate Agreement between the practice and each Business Associate must:

◆ Establish the permitted and required uses and disclosures of PHI by the Business Associate.

◆ Provide that the Business Associate will not use or further disclosure the PHI other than as permitted or required by the contract or as required by law.

◆ Require the Business Associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing the requirements of the Security Rule, with regard to electronic PHI.

◆ Require the Business Associate to report to the practice any use or disclosure of the information not provided for under the contract, including incidents that constitute breaches of unsecured PHI.

◆ Require the Business Associate to disclosure PHI as specified in the contract to satisfy the practice's obligation with respect to PHI, as well as make available PHI for amendments (and incorporate any amendments, if required) and accountings.

◆ To the extent that a Business Associate is to carry out the practice's obligations under the Privacy Rule or the Security Rule, require the Business Associate to comply with the specific requirements applicable to these obligations.

◆ Require the Business Associate to make available to HHS its internal practice, books, and records relating to the use and disclosure of PHI received from, or created or received by the Business Associate on behalf of, the practice, for purposes of HHS' determination of the practice's compliance with the Privacy Rule and the Security Rule.

◆ At termination of the contract, if feasible, require the Business Associate to return or destroy all PHI received from, or created or received by the Business Associate on behalf of, the practice.

◆ Require the Business Associate to ensure that any subcontractors it may engage on its behalf that will have access to PHI agree to the same restrictions and conditions that apply to Business Associates with respect to such information.

◆ Authorize termination of the contract by the practice if the Business Associate violates a material term of the contract. (Contracts between Business Associates and its subcontractors should also have this same requirement).

To do:

• Fill in the Practice Name on Exhibit 17.

• Once identified, the Privacy Officer should meet, if possible, with each Business Associate. If a meeting is not feasible, then the Privacy Officer can discuss via the telephone the Business Associate Agreement. The Privacy Officer should provide the Business Associate with a contract and request his/her signature.

• Require the Business Associate to provide names of their employees or representatives who may enter the practice and/or have access to PHI.

Notes:

• Covered entities are not Business Associates when providing treatment. However, if a covered entity is providing non-treatment services, such as billing, for the practice, then it is acting in this situation as a Business Associate. Thus it is not covered by the Privacy Rule and needs a Business Associate Agreement.

• As noted, Business Associates are directly liable under HIPAA for their own violations. However, medical practices can still be held liable for the privacy violations of their Business Associates, should the Business Associate be considered an agent of the practice.

Step 20: Train All Physicians and Staff on Privacy Policies and Notice of Privacy Practices

See Exhibit 18 for Your Privacy Policy Training Checklist.

All physicians and staff (your workforce) must be trained on the practice's Privacy Policies and Notice of Privacy Practices and how they affect their individual job responsibilities. Your Privacy Training Checklist is provided in Exhibit 18 to assist your Privacy Officer in conducting the privacy training.

To do:

• Fill in Practice Name on Exhibit 18.

• Photocopy the Privacy Policy Training Checklist as needed for each training session conducted.

• The Privacy Officer must review and revise, if necessary, all training materials. The introduction to this manual and many of the exhibits in it may be used as training tools for physicians and staff.

• Schedule the first training session for all currently employed physicians and staff, as well as other workforce members, such as volunteers.

• Employees should be encouraged to ask questions during the training or at any future date in the event of confusion or questions regarding the Privacy Policies.

• Modify the new employee orientation checklist to include time set aside for Privacy Policy training.

• All new employees are required to receive privacy training as a part of their initial employee orientation.

• Any time there is a material change in the Privacy Policy that affects your practice and how your staff conducts business, the employees whose functions and responsibilities are affected by the change are required to receive additional training.

• Records of physician and staff Privacy Policy training must be maintained for six (6) years.

• Physicians and staff should receive follow-up training on a routine basis.

Step 21: Document Physician and Staff Training

See Exhibit 19 for Your Training Documentation Form.

All physicians and staff should be given a copy of the practice's Privacy Policies and Procedures and should sign it as proof that they have reviewed and understand it.

In addition, all physician and staff training on the Privacy Policies and Procedures must be documented.

To do:

• Fill in Practice Name on Exhibit 19.

• Photocopy the Training Documentation Form as needed for each training session conducted.

• After the training session, have physicians and staff record their names, titles and signatures.

• This form should be maintained by the Privacy Officer.

• Modify new employee orientation checklist to make certain that the employee has signed the Training Documentation form.

Notes:

• Employees may sign training documentation forms individually. Upon signature, the forms should be placed in their personnel file.

• Document any additional training and training of new employees in the same manner.

• Records of the HIPAA Privacy Policy training must be maintained for six (6) years.

Step 22: Obtain Signed Workforce Confidentiality Agreements from All Physicians and Staff

See Exhibit 20 for Your Sample Workforce Confidentiality Agreement.

Although the Privacy Rule does not require employees to sign a confidentiality agreement, the Rule does require a practice to implement policies and procedures relating to PHI. Further, the Rule does require a practice to train their workforce members regarding such policies and procedures.

As a suggestion, all employees (including physicians) should sign a Workforce* Confidentiality Agreement. This agreement requires the employee to keep all PHI confidential. The signed agreement will (if followed and enforced) substantiate your practice's training and compliance efforts and may assist in the lessening of any penalties imposed in the event of a violation of the Privacy Rule.

To do:

• Fill in Practice Name on Exhibit 20.

• Photocopy the Workforce Confidentiality Agreement.

• Distribute the Workforce Confidentiality Agreement to physicians and staff.

• Collect a signed agreement from physicians and staff and return them to the Privacy Officer.

• Revise practice's new employee orientation checklist to include the following step: "Sign your practice's Workforce Confidentiality Agreement."

• Place signed agreement in employee's personnel file.

Notes:

• State laws may vary regarding use of the Workforce Confidentiality Agreement as a condition for new or continued employment. Consult with your attorney prior to the use/enforcement of the agreement in your jurisdiction.

• Since this is a new policy of the practice, all current employees should sign one of these agreements. In the future, the signing of this agreement should be part of the orientation for all new employees.

**Workforce includes physicians, other providers, employees (full-time and part-time) and volunteers.*

Step 23: Monitor Compliance with the Privacy Rule

See Exhibit 21 for the Privacy Officer's Incident Event Log.

It is the responsibility of the Privacy Officer to monitor the practice's compliance with the Privacy Rule, including compliance with the practice's breach notification responsibilities. The Privacy Officer should encourage all physicians and staff to communicate openly with him/her concerning any potential privacy breaches or to provide recommendations for how the practice could be better organized to protect patients' confidentiality. Note that no physician, provider or staff member is immune from adhering to the Privacy Rule.

If staff are aware of a possible violation of the Privacy Rule that involves the Privacy Officer, then the communication should be made to a physician owner, the president of the practice, or another individual in a leadership capacity.

To do:

• Fill in Practice Name on Exhibit 21.

• The Privacy Officer should create processes to monitor compliance. This may include periodic walk-throughs of the practice and/or may include spot checks.

• The Privacy Officer should offer a mechanism by which staff can address privacy concerns.

Notes:

• An Event Log or sufficient similar documentation should be maintained by the Privacy Officer to record the receipt of complaints concerning the practice's Privacy Policies and Procedures required by the Privacy Rule, or its compliance with its Policies and Procedures. The log should include the follow-up on all privacy complaints.

• Take appropriate actions on all possible violations of policy in accordance with the practice's Privacy Policies and Procedures.

• Appropriate measures need to be taken by the Privacy Officer to prevent violations or potential violations of the Privacy Rule from occurring again. The practice must have and apply appropriate sanctions against members of its workforce who fail to comply with the practice's Privacy Policies and Procedures or the Privacy Rule.

• The practice must document any sanctions/discipline applied to its employees/workforce members and retain such records for six (6) years.

Step 24: Breach Notification Requirements

See Exhibits 22, 23 and 24 for a Breach Notification Policy, Letter and Log.

A covered entity must know what to do if there is a breach of unsecured PHI. A breach is presumed to have occurred when PHI is acquired, accessed, used or disclosed in a manner not permitted under HIPAA, unless it is demonstrated that there is a "low probability that the PHI has been compromised," as determined by a risk assessment.

To understand what a breach is, it is helpful to start by noting what is not a breach. The following are not considered breaches:

i. an unintentional use of PHI by a workforce member of the Covered Entity or Business Associate acting in good faith and within the scope of his or her authority, and the PHI is not further improperly used and disclosed;

ii. an inadvertent disclosure of PHI by an authorized person to another authorized person at the same Covered Entity or Business Associate, and the PHI is not further improperly used and disclosed; and

iii. a disclosure of PHI to an unauthorized person where there is a good faith belief that the disclosed PHI could not be retained.

If any of these exceptions apply, no breach has occurred and the practice is not required to notify any patients.

Also, no breach is deemed to have occurred if there is a low probability that PHI has been compromised, as determined by a risk assessment. The risk assessment must include all of the following factors:

i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

ii. The unauthorized person who used the PHI or to whom the disclosure was made;

iii. Whether the PHI was actually acquired or viewed; and

iv. The extent to which the risk to the PHI has been mitigated.

The risk assessment must also be completed in good faith, and the practice's conclusions should be reasonable in light of the factual circumstances surrounding the unauthorized acquisition, use, access or disclosure.

If the practice performs a risk assessment and determines that there is more than a low probability that the PHI has been compromised as a result of the unauthorized acquisition, access, use or disclosure of unsecured PHI, then breach notification is required.

Notifications must be made no later than sixty (60) days after discovering the breach. A breach is considered "discovered" on the first day the breach is known or "by exercising reasonable diligence would have been known."

If a breach is discovered by one of the Business Associates of the practice, the Business Associate must notify the practice within sixty (60) days of the first day the breach is discovered. However, consider the practical implications. The practice must notify an affected patient within sixty (60) days of discovery of the breach. If a Business Associate has this same time frame to notify the practice, the practice might not be able to meet its own 60 day deadline. Therefore, it's advisable for the Business Associate Agreement to provide a shorter timeframe (e.g. 30 days) for the Business Associate to notify the practice. For existing vendors, this can be accomplished by amending the existing Business Associate Agreement to reflect the shorter timeframe.

The practice's written notification to affected patients must include the following:

1. a brief description of what happened, including the date of the breach and the date of discovery, if known;

2. a description of the types of unsecured PHI that were involved;

3. any steps the patient should take to protect himself or herself from potential harm resulting from the breach;

4. a brief description of what the practice is doing to investigate, mitigate, and protect against future breaches; and

5. the practice's contact information so the patient may obtain additional information, if needed.

Notifications must be in writing and sent via first class mail to the patient at his or her last known address or by e-mail if the patient has consented to receiving electronic communications from the practice. If the patient is deceased, then the notification must be sent to the address of the patient's personal representative or next of kin. If the information the practice has on file is insufficient or out of date, then notice may be sent by substitute form if the practice believes it will reasonably reach the patient. A substitute form of notification to less than ten (10) patients may be a phone call or e-mail. A substitute form of notification to ten (10) or more patients may be a notice posted on the practice's website. This posted notice must remain up for ninety (90) days and must provide patients with a toll-free number so that they can obtain additional information about the breach. In urgent situations, the practice may contact the affected patient by phone or other means. The practice should be sure to follow up with a written notice to the patient or his or her representative.

The Secretary of HHS must be notified of any breaches that are discovered during the calendar year within sixty (60) days of the calendar year end. This means that the practice must keep an ongoing log of any breaches that are discovered throughout the year so that it can accurately report to HHS at year end. If the breach involves more than 500 residents of the United States, the practice must immediately notify prominent media outlets and the Secretary of HHS. The media outlets to be notified are those television stations and newspapers local to the area in which the practice is located or the areas from which the practice draws patients.

Note that the breach, depending on its nature, may have implications under state privacy or other state or federal laws. For example, both California and Pennsylvania have laws which against the disclosure of "personal information", which includes information such as driver's license numbers and social security numbers. If substance abuse records are compromised, the practice will have to deal with the federal Public Health Services Act. There could be issues on both the state and federal level with identity theft if Social Security numbers are involved, and general tort law theories (intentional or negligent infliction of emotional distress) if there is an improper disclosure of a disease or condition. In situations where a breach of these types of records has occurred, the practice should contact its local legal counsel immediately for further advice on how to handle the notifications.

Keep in mind that the practice's notice demonstrates that it has made good faith attempt to inform the patient, and do damage control. This is important if there is any government investigation that occurs. Remember, the burden of proof is on the Practice to demonstrate that all required notifications have been provided.

In limited situations, notice may be delayed for a specified period of time. Notice must be delayed if law enforcement states to the practice that such notification would "impede a criminal investigation or cause damage to national security." If the statement is made in writing and specifies the period of time for delay, the practice must delay notification for that period of time. If the statement is made verbally, notification may be delayed for no more than thirty (30) days from the verbal statement. All verbal statements should be documented and confirmed in writing.

EXHIBITS

Exhibit 1: Privacy Officer Job Responsibilities

_____
Practice Name

The Privacy Officer for this practice oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the practice's policies and procedures related to the privacy of and access to patients' protected health information (PHI) in compliance with federal and state laws and the practice's privacy practices, including its breach notification policies (collectively, the "Privacy Policy").

Responsibilities:

◆ Maintain current knowledge of applicable federal and state privacy laws.

◆ Develop, oversee and monitor implementation of the practice's Privacy Policy and ensure that the integrity of the Privacy Policy is maintained at all times.

◆ Report regularly to the practice governing body and officers (as applicable) regarding the status of the Privacy Policy.

◆ Work with legal counsel, management and committees to ensure that the practice maintains appropriate privacy consent and authorization forms, notices and other administrative materials in accordance with practice management and legal requirements.

◆ Establish and administrate a process for receiving, documenting, tracking, investigating and taking action on all complaints concerning the practice's privacy policies and procedures in coordination and collaboration with other similar functions, and, when necessary, with legal counsel.

◆ Establish and oversee practice policies for addressing patient requests to obtain or amend patient records or to obtain accountings of disclosures; ensure compliance with practice policies and legal requirements regarding such requests and establish and oversee grievance and appeals processes for denials of requests related to patient access or amendments.

◆ Oversee, direct, deliver, or ensure the delivery of privacy training and orientation to all employees, volunteers, medical and professional staff, and other appropriate personnel and maintain appropriate documentation of privacy training.

- Monitor attendance at all Privacy Policy training sessions and evaluate participants' comprehension of the information provided at training sessions.
- Monitor compliance with Privacy Policy including periodic privacy risk assessments.
- Establish benchmarks to evaluate, on no less than an annual basis, the Privacy Policy's success in meeting the practice's goal for protection of PHI.
- Coordinate and participate in disciplinary actions related to the failure of practice workforce members to comply with the practice Privacy Policy and/or applicable law.
- Monitor technological advancements related to protected health information protection and privacy for consideration of adaptation by the practice.
- Coordinate and facilitate the allocation of appropriate resources for the support of and the effective implementation of the Privacy Policy.
- Initiate, facilitate and promote activities to foster privacy information awareness within the practice.
- Cooperate with the Office of Civil Rights, other legal entities, and practice officers in any compliance reviews or investigations.
- Perform periodic risk assessments and ongoing compliance monitoring activities at each practice location.
- Act as point of contact for practice legal counsel in an ongoing manner and in the event of a reported violation.
- Maintain all business associate contracts and respond appropriately if problems arise.
- Act as the practice-based point of contact for receiving, documenting and tracking all complaints concerning privacy policies and procedures of the practice.

Skills:

- Able to facilitate change.
- Possess knowledge and understanding of privacy law and technology.

Exhibit 2: Internal Privacy Checklist

_____
Practice Name

_____
Date

Conduct a "walk-through" of the practice to identify areas where non-authorized individuals (patients and others) potentially have access to patients' medical and non-medical Protected Health Information (PHI).

Begin by walking through your practice's front door and review the current procedure relating to the questions below. So as to avoid missing any area of the practice, all potential areas of a practice are listed here. ***Note: Some steps may repeat, some may not be relevant to your practice.*** The "Action Needed" area is your practice's determination of the opportunity to describe efforts to comply with the Privacy Rule. Actions should be described in detail and should include the responsible person and target completion date.

Many of these tasks relate to the minimum necessary standard described in the Privacy Rule (see page 17 of the manual). According to the OCR HIPAA Privacy Guidance, the minimum necessary standard "is not a strict standard and Covered Entities need not limit information uses or disclosures to those that are absolutely needed to serve the purpose. Rather, this is a reasonableness standard that calls for an approach consistent with the suggestions and guidelines already used by many providers today to limit the unnecessary sharing of medical information." ***In other words — common sense should be a major guidance. Practices are not expected to reconstruct existing facilities.***

Front Office/Check-In

	Review of Current Procedure	HIPAA Citation	Guidelines for Policy Adherence*	Action Needed to be Taken/Responsible Person/Date Completed
Task 1	Does the practice utilize a patient sign in sheet?	164.530 (c)(1)	HHS does not intend to prohibit the use of sign-in sheets. The "minimum necessary" standard should be followed with sensitivity toward protecting individual health information (e.g., limit the sign-in sheet to the patient's name and date). (Suggestion)	
Task 2	How does the practice obtain verification from an established patient that his/her demographic and insurance information is still accurate?	164.530 (c)(1)	Have check-in receptionist provide a printed copy of patient's demographic and insurance information to the patient for his/her review. Request that the patient note any changes prior to returning it to the check-in receptionist. (Suggestion)	
Task 3	If it is necessary for check-in staff to request verbal clarification of patient-related information, is a private area readily available to protect the patient's privacy during the verbal exchange (e.g., a cubicle or separate office)?	164.530 (c)(1)	Voices should be kept down so that the conversation cannot be overheard easily by non-authorized persons. Alternatively, a private area should be established for staff to discuss PHI with patients in order to adhere to the minimum necessary release of information standard. (Suggestion)	

continued

These Guidelines for Policy Adherence may not be explicitly stated in the Privacy Rule. Some are based on our interpretation of the "minimum necessary" standard and our experience in practice management. If stated in the Privacy Rule, it is so indicated by the notation (Regulation) at the end of the Guidelines, otherwise the notation (Suggestion) follows.

Front Office/Check-In (continued)

	Review of Current Procedure	HIPAA Citation	Guidelines for Policy Adherence*	Action Needed to be Taken/Responsible Person/Date Completed
Task 4	Are printouts of the appointment schedule in plain view of patients (e.g., on the front office counter, in the nurse's station, lab, etc.)?	164.530 (c)(1)	Appointment schedules should be placed out of sight from patients and other non-authorized persons in order to protect patient confidentiality. Examples of ways to keep these out of sight, yet easily accessible include placing them in an opaque binder or a drawer or access it on a computer screen that is not visible to others. (Suggestion)	
Task 5	Are computer screens visible to patients in the waiting area?	164.530 (c)(1)	Computer screens should be facing away from patients and non-authorized individuals. As an alternative, screen covers that allow only straight-on viewing can be used in order to protect patient confidentiality. (Suggestion)	
Task 6	A. If the practice maintains a website, is the practice's Notice of Privacy Practices prominently placed on the site and available for viewing? B. Is the patient provided with a copy of the practice's Notice of Privacy Practices describing the practice's uses and disclosures of PHI? C. Is written acknowledgement of receipt of the Notice of Privacy Practices obtained from the patient? D. Is the practice's Notice of Privacy Practices posted? If so, where?	164.520 (c)	See Exhibits 3 and 4 and Steps 5 and 6. (Regulation)	

continued

These Guidelines for Policy Adherence may not be explicitly stated in the Privacy Rule. Some are based on our interpretation of the "minimum necessary" standard and our experience in practice management. If stated in the Privacy Rule, it is so indicated by the notation (Regulation) at the end of the Guidelines, otherwise the notation (Suggestion) follows.

Front Office/Check-In (continued)

	Review of Current Procedure	HIPAA Citation	Guidelines for Policy Adherence*	Action Needed to be Taken/Responsible Person/Date Completed
Task 7	How are patients called to the exam/treatment area (e.g., by first name only, first and last name, last name only, number system, photo id)?	164.530 (c)(1)	To protect patient confidentiality, practices may wish to avoid using both first and last names together, and instead use either just first name or just last name when calling patients back for treatment or use. (Suggestion)	
Task 8	A. Are messages left on answering machines/ voice mails? B. Are postcards used to remind patients of appointments? C. Do invoices or other correspondence to patients reflect on the exterior envelope the nature of the practice (for example, "Oncology Specialists" or "Psychological Counseling"?)	164.506 (a)(1)	Unless patients fill out a restriction form (see Step 9 and Exhibit 8) requesting a reasonable alternative means of communication or an alternative location at which to be contacted, practices may call patients and leave messages on answering machines/voicemails. Preferably, postcards should not be used to remind patients of appointments. Correspondence to patients should be labeled "Personal and Confidential" and if at all possible should not identify the nature of services offered by the practice. (Suggestion)	
Task 9	Does the practice treat personal representatives of adults, unemancipated minors (parents, guardians and other persons acting in loco parentis) and deceased persons (executor, administrator, etc.) as it would an individual?	164.502 (g)(1)	See Step 1, Personal Representatives under HIPAA (pages 27 and 28). Please refer to your state's specific requirements as state law that provides greater rights to patients or greater privacy protection apply. (Regulation)	

These Guidelines for Policy Adherence may not be explicitly stated in the Privacy Rule. Some are based on our interpretation of the "minimum necessary" standard and our experience in practice management. If stated in the Privacy Rule, it is so indicated by the notation (Regulation) at the end of the Guidelines, otherwise the notation (Suggestion) follows.

Clinical Area (includes exam rooms, treatment and procedure rooms, lab, radiology and common areas adjacent to these areas)

	Review of Current Procedure	**HIPAA Citation**	**Guidelines for Policy Adherence***	**Action Needed to be Taken/Responsible Person/Date Completed**
Task 1	**Do providers and/or staff members discuss or dictate patient information or talk on the phone in close proximity to public areas where they might be overheard by patients and non-authorized individuals (e.g., nurses station, outside exam rooms or other treatment areas, waiting room, front office area)?**	**164.530 (c)(1)**	While this is permitted, discretion should be exercised that these conversations occur in such a way as to minimize the risk of being overheard by non-authorized individuals. (Suggestion)	
Task 2	Are exam room doors left open during a patient exam visit?	164.530 (c)(1)	Ideally, exam room doors should be closed while a provider is examining a patient or discussing PHI with a patient. (Suggestion)	
Task 3	Are providers using the telephone in a patient occupied exam room to discuss other identifiable patients' information?	164.530 (c)(1)	Providers should not take phone calls pertaining to patients while in an occupied exam room occupied by patients, especially if the other patient can or might be identified. (Suggestion)	
Task 4	Are lab and x-ray logs and similar documents viewable or accessible by non-authorized personnel?	164.530 (c)(1)	All lab and x-ray logs and related documents should be stored in areas that are not visible or accessible to non-authorized individuals. These documents should be secured when not in use. (Suggestion)	
Task 5	Are x-ray folders, or lab requisition requests and/or similar material bearing PHI visible?	164.530 (c)(1)	All x-ray folders, lab requisition requests and/or similar materials bearing PHI should be utilized so as not to be visible to non-authorized individuals. These materials should be secured when not in use. (Suggestion)	
Task 6	In route to and from exam room or treatment areas, do patients pass unattended through areas where medical charts or other	164.530 (c)(1), (i)(1) 164.514 (d)(1)	Incidental disclosures do not violate the Privacy Rule but PHI (other than name) should not be visible or otherwise accessible to anyone other than practice personnel requiring the	

continued

	Review of Current Procedure	**HIPAA Citation**	**Guidelines for Policy Adherence***	**Action Needed to be Taken/Responsible Person/Date Completed**
	patient related information are in plain view and accessible by non-authorized individuals?		minimum necessary information to perform treatment, payment or healthcare operations for the practice. (Regulation)	

These Guidelines for Policy Adherence may not be explicitly stated in the Privacy Rule. Some are based on our interpretation of the "minimum necessary" standard and our experience in practice management. If stated in the Privacy Rule, it is so indicated by the notation (Regulation) at the end of the Guidelines, otherwise the notation (Suggestion) follows.

Front Office/Check-Out

	Review of Current Procedure	**HIPAA Citation**	**Guidelines for Policy Adherence***	**Action Needed to be Taken/Responsible Person/Date Completed**
Task 1	Does the practice have a private or semi-private area to conduct financial counseling, set-up payment plans and schedule surgeries or procedures, etc. (e.g., cubicle or separate office)?	164.530 (c)(1)	The practice should have an area available to discuss confidential information with patients where PHI cannot easily be overheard by non-authorized individuals. (Suggestion)	
Task 2	Are computer screens visible to patients and non-authorized individuals?	164.530 (c)(1)	Computer screens should face away from patients and non-authorized individuals and towards staff. Screens/covers that allow only straight-on viewing may be used. (Suggestion)	
Task 3	Are encounter forms and/or other patient paperwork (e.g., walkout statement) visible to patients and/or non-authorized individuals?	164.530 (c)(1)	Encounter forms and other patient paperwork should be kept out of sight from non-authorized individuals in order to protect patient confidentiality. (Suggestion)	

These Guidelines for Policy Adherence may not be explicitly stated in the Privacy Rule. Some are based on our interpretation of the "minimum necessary" standard and our experience in practice management. If stated in the Privacy Rule, it is so indicated by the notation (Regulation) at the end of the Guidelines, otherwise the notation (Suggestion) follows.

Front Office/General

	Review of Current Procedure	HIPAA Citation	Guidelines for Policy Adherence*	Action Needed to be Taken/Responsible Person/Date Completed
Task 1	Does the practice have protocols for verifying that a patient contacting the practice or a patient contacted by the practice via telephone for appointment scheduling, collections activities, communicating lab results, etc. is actually the patient in question?	164.530 (c)(1)	The patient identity should be verified by DOB, social security number, mother's maiden name, PIN or other unique identifier. The patient should provide this confirming information, not the practice. (Suggestion)	
Task 2	If PHI is received in the office via facsimile, is the fax machine located in a non-public, secure area?	164.530 (c)(1)	Fax machines should be located away from areas where patients or other non-authorized individuals may be present or have visual access. (Suggestion)	
Task 3	Does the practice verify that outgoing faxes are going to the appropriate party and confirming fax numbers of recipients?	164.530 (c)(1)	Only parties authorized to receive PHI under applicable law and the practice's privacy policies should receive PHI via fax. All fax numbers should be confirmed prior to dialing, or use autodial features. (Suggestion)	
Task 4	Are staff and/or providers logging out of all software programs prior to leaving computer terminal unattended?	164.530 (c)(1)	All providers and staff should log out of all programs containing PHI prior to leaving a computer terminal unattended. The use of a password protected screensaver is another viable alternative. (Suggestion)	
Task 5	Are all staff members provided with unique passwords for program access?	164.530 (c)(1) 164.514 (d)(1)	Each staff member and provider should immediately be provided with his/her own password that allows him/her access to PHI at levels required by his/her job description in order to adhere to the minimum necessary standard. (Suggestion)	

These Guidelines for Policy Adherence may not be explicitly stated in the Privacy Rule. Some are based on our interpretation of the "minimum necessary" standard and our experience in practice management. If stated in the Privacy Rule, it is so indicated by the notation (Regulation) at the end of the Guidelines, otherwise the notation (Suggestion) follows.

Medical Records

	Review of Current Procedure	HIPAA Citation	Guidelines for Policy Adherence*	Action Needed to be Taken/Responsible Person/Date Completed
Task 1	Who is authorized to access and/or remove medical records?	164.514 (d)(2)(B)	Define those authorized and permit only the personnel whose job description states that they need access to medical records to remove and file charts. See Step 16. (Regulation)	
Task 2	When medical records are removed from the filing system, is there a tracking mechanism in place to document the charts' location?	164.530 (c)(1)	A tracking mechanism such as outguides or other devices should be used to track the whereabouts of medical records to aid in ensuring that PHI is only in authorized areas. (Suggestion)	
Task 3	Has the practice determined the physical means of maintaining medical records so that they meet the privacy and security requirements?	164.530 (c)(1)	Medical records must be kept private and secure. (Regulation) A suggestion would be to have an area for charts to be locked after hours. Another alternative would be to obtain a confidentiality agreement with after-hours service providers. (Suggestion)	
Task 4	Are medical records transported between locations? (If applicable)	164.530 (c)(1)	Only PHI that is necessary for carrying out TPO should be transported to satellite locations. (Information needed should be copied, if possible, to prevent misplacing patients' medical record.) Note: If a courier is used, the PHI should not be visible/accessible to the courier. A suggestion would be to use a lock bag with couriers. Otherwise, be certain that a Business Associate Agreement is in place with the courier. (Suggestion)	
Task 5	Does the practice have a process for using and disclosing PHI?	164.530 (c)(1)	See Exhibits 3, 5 and 5A. (Regulation)	
Task 6	Is a patient's written authorization obtained (as appropriate) prior to releasing PHI for purposes other than TPO?	164.508 (a)	See Exhibits 6, 7 and Step 8. (Regulation)	
Task 7	Are signed authorizations to disclose PHI for reasons other than treatment, payment or healthcare operations (TPO) maintained in each patient's medical record?	164.508 (a)	See Exhibits 6, 7 and Step 8. (Regulation)	

continued

	Review of Current Procedure	**HIPAA Citation**	**Guidelines for Policy Adherence***	**Action Needed to be Taken/Responsible Person/Date Completed**
Task 8	Does the practice document disclosure activity regarding non-TPO uses and disclosures of PHI? Is this tracking information available in a format that can be easily provided to a patient?	164.528 (a)	See Exhibit 13 and Step 14. (Regulation)	
Task 9	Does the practice have staff members who are trained to respond to patient's requests regarding their own PHI?	164.530 (a)(1)(ii)	The practice must have at least one staff member who is knowledgeable and responsive to patients' inquiries about exercising their rights to restrict, amend, and obtain copies of or an accounting of disclosures of their PHI. (Regulation)	
Task 10	Does the practice contract with an outside vendor for the destruction of medical records that should be purged?	164.514 (b)(1)(i) 164.504 (e)	The practice should have a Business Associate Agreement with third party vendors who have access to PHI. See Exhibit 17 and Steps 18 and 19. (Regulation)	
Task 11	When PHI is destroyed, is it burned, shredded or otherwise rendered unreadable?		PHI must be rendered unreadable when it is destroyed. Consider using a shredder to destroy documents. (Suggestion)	
Task 12	If psychotherapy notes are retained in the patient record, are they segregated or identified so as to easily preclude unauthorized dissemination?	164.524 (a)(1)(i)	Any release of psychotherapy notes require an authorization. (Regulation)	
Task 13	Does the practice communicate with patients via e-mail?	164.530 (i)(1)	The practice should obtain the patient's permission and should consider using encryption for e-mail messages between the practice and its patients. The practice should establish policies to authenticate the recipients and senders of e-mail containing PHI. (Suggestion)	
Task 14	Does the practice post PHI to their web site and allow patient access? (e.g., lab results, x-ray results, etc.)	164.530 (c)(1)	This web site must be secured with access to PHI given only to the appropriate patient via a password. (Suggestion)	
Task 15	Do the providers take medical records out of the practice?	164.530 (c)(1)	Except in emergencies related to patient care, providers should not take medical records out of the practice. The information that is taken out of the practice should be limited to only that which is needed to care for the patient. (Suggestion)	

continued

	Review of Current Procedure	HIPAA Citation	Guidelines for Policy Adherence*	Action Needed to be Taken/Responsible Person/Date Completed
Task 16	Does the practice have a mechanism for de-identification of PHI?	164.514 (b)(1)	See Appendix 7 for what to do in research situations. (Regulation)	
Task 17	Does the practice engage in marketing? For example, does the practice participate in activities such as mailing patients information about health prevention or promotion activities?	164.508(a)(3)	See Step 1 overview section related to marketing. (Regulation)	
Task 18	Are deceased patients' records treated according to the same policy as current patients' records?	164.502 (f)	Deceased patients' records are subject to the same rules as all living patients; however, this requirement applies only for a period of fifty (50) years following the death of the individual. (Regulation)	

These Guidelines for Policy Adherence may not be explicitly stated in the Privacy Rule. Some are based on our interpretation of the "minimum necessary" standard and our experience in practice management. If stated in the Privacy Rule, it is so indicated by the notation (Regulation) at the end of the Guidelines, otherwise the notation (Suggestion) follows.

Business Office

	Review of Current Procedure	HIPAA Citation	Guidelines for Policy Adherence*	Action Needed to be Taken/Responsible Person/Date Completed
Task 1	Are calls in which PHI is discussed made in close proximity to public areas where they might be overheard by non-authorized individuals?	164.530 (c)(1)	Phone calls in which PHI is disclosed should ideally be made in private areas. (Suggestion)	
Task 2	Are computer screens visible to patients?	164.530 (c)(1)	Computer screens should be facing away from patients and non-authorized individuals and towards staff or have screen covers that allow only straight-on viewing in order to protect patient confidentiality. (Suggestion)	
Task 3	Are printouts of patients' financial and/or insurance information (e.g., EOBs, incoming and outgoing mail, patient and insurance checks) in plain view of patients or other non-authorized individuals?	164.530 (c)(1)	PHI should not be visible by non-authorized individuals in order to protect patient confidentiality. (Suggestion)	

continued

	Review of Current Procedure	HIPAA Citation	Guidelines for Policy Adherence*	Action Needed to be Taken/Responsible Person/Date Completed
Task 4	In collection efforts, are messages left on patient answering machines or voice mails or are services apparent externally on mailings?	164.506 (a)	In general, a practice can leave messages on patient answering machines or voicemails in regards to collection efforts unless the patient completes the Request for Limitations and Restrictions of PHI Form (Exhibit 8) and instructs the practice to not do so. Ideally, calls should be made out of hearing range of patients or other non-authorized individuals. Envelopes to patients should be labeled "personal and confidential" and if at all possible should not identify the nature of services offered by the practice. (Suggestion)	

These Guidelines for Policy Adherence may not be explicitly stated in the Privacy Rule. Some are based on our interpretation of the "minimum necessary" standard and our experience in practice management. If stated in the Privacy Rule, it is so indicated by the notation (Regulation) at the end of the Guidelines, otherwise the notation (Suggestion) follows.

Business Associate

	Review of Current Procedure	HIPAA Citation	Guidelines for Policy Adherence*	Action Needed to be Taken/Responsible Person/Date Completed
Task 1	Are signed business associates agreements in place, if the practice utilizes any of the following and the entity needs access to PHI to perform services for the practice?	164.504 (e)(1), (2)	See Exhibits 15, 16 and 17 and Steps 18 and 19. (Regulation)	
Task 2	How do Business Associates identify themselves when visiting the practice (e.g., badge, business card, driver's license)?	164.530 (c)(1)	Business Associate identities should be verified prior to giving access to the practice and PHI, in order to protect patient confidentiality. (Suggestion)	

These Guidelines for Policy Adherence may not be explicitly stated in the Privacy Rule. Some are based on our interpretation of the "minimum necessary" standard and our experience in practice management. If stated in the Privacy Rule, it is so indicated by the notation (Regulation) at the end of the Guidelines, otherwise the notation (Suggestion) follows.

Personnel

	Review of Current Procedure	HIPAA Citation	Guidelines for Policy Adherence*	Action Needed to be Taken/Responsible Person/Date Completed
Task 1	Does the practice have written Privacy Policies and Procedures in place?	164.530 (i)(1)	The practice must have written Privacy policies and procedures included in their policies and procedures manual. See Exhibits 5 and Step 7. (Regulation)	
Task 2	Are the practice's privacy policies and procedures periodically reviewed and updated? If so, how often? • If so, by whom? • If so, when were they most recently updated?	164.530 (i)(2)	The practice should review their privacy policies and procedures at least annually and must update them as required if there are changes to the Privacy Rule. (Regulation)	
Task 3	Do new employees receive privacy training as part of their new employee orientation? Have all existing employees undergone training?	164.530 (b)(1)	See Exhibit 18 and Step 20. (Regulation)	
Task 4	Has new employee privacy training taken place? Is it documented?	164.530 (b)(2)(ii)	See Exhibit 19. (Regulation)	
Task 5	Does every practice employee have a signed workforce confidentiality agreement in his/her personnel file?		See Exhibit 20 and Step 22. (Suggestion)	
Task 6	Does someone in the practice have privacy duties as a part of their job description? Is it in writing?	164.530 (a)(1)	See Exhibit 1 and Step 2. (Regulation)	
Task 7	Have incidents occurred in which patient privacy was breached?	164.530 (i)(1)	The practice should follow its Privacy Policies and Procedures to prevent breaches from occurring. (Regulation)	
Task 8	Is the practice adhering to its Privacy Policy for documenting and following up on patient privacy breaches?	164.530 (d)(2) 164.530 (i)(1)	See Exhibit 21 and Step 23. (Regulation)	
Task 9	Upon the occurrence of a breach of the practice's privacy	164.530 (d)(2) & 164.400 and following sections	The reason for the privacy breach should be identified. (Suggestion)	

continued

	Review of Current Procedure	**HIPAA Citation**	**Guidelines for Policy Adherence***	**Action Needed to be Taken/Responsible Person/Date Completed**
	policies, were the protocols of the practice's Breach Notification Policy followed? Both in terms of internal notifications and external notifications? Was the reason for the breach identified?			
Task 10	Have measures been taken to prevent similar instances from occurring in the future?	164.530 (i)(1)	When a privacy breach has occurred, a practice must put appropriate measures in place to prevent a similar privacy breach from occurring again. See Exhibit 21. (Suggestion)	

These Guidelines for Policy Adherence may not be explicitly stated in the Privacy Rule. Some are based on our interpretation of the "minimum necessary" standard and our experience in practice management. If stated in the Privacy Rule, it is so indicated by the notation (Regulation) at the end of the Guidelines, otherwise the notation (Suggestion) follows.

Exhibit 3: Notice of Privacy Practices

THIS DOCUMENT IS A TEMPLATE ONLY. IT DOES NOT REFLECT THE REQUIREMENTS OF YOUR STATE'S LAWS. YOU SHOULD CONSULT WITH ADVISORS (YOUR STATE OR LOCAL MEDICAL OR SPECIALTY SOCIETY, ASSOCIATION OR LEGAL OR OTHER COUNSEL) FAMILIAR WITH YOUR STATE'S PRIVACY LAWS PRIOR TO USING THIS DOCUMENT.

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION

PLEASE READ IT CAREFULLY

The Health Insurance Portability & Accountability Act of 1996 ("HIPAA") is a Federal program that requests that all medical records and other individually identifiable health information used or disclosed by us in any form, whether electronically, on paper, or orally are kept properly confidential. This Act gives you, the patient, the right to understand and control how your personal health information ("PHI") is used. HIPAA provides penalties for covered entities that misuse personal health information.

As required by HIPAA, we prepared this explanation of how we are to maintain the privacy of your health information and how we may disclose your personal information.

We may use and disclose your medical records only for each of the following purposes: treatment, payment and health care operation.

- Treatment means providing, coordinating, or managing health care and related services by one or more healthcare providers. An example of this is a primary care doctor referring you to a specialist doctor.

- Payment means such activities as obtaining reimbursement for services, confirming coverage, billing or collections activities, and utilization review. An example of this would include sending your insurance company a bill for your visit and/or verifying coverage prior to a surgery.

- Health Care Operations include business aspects of running our practice, such as conducting quality assessments and improving activities, auditing functions, cost management analysis, and customer service. An example of this would be new patient survey cards.

- The practice may also be required or permitted to disclose your PHI for law enforcement and other legitimate reasons. In all situations, we shall do our best to assure its continued confidentiality to the extent possible.

We may also create and distribute de-identified health information by removing all reference to individually identifiable information.

We may contact you, by phone or in writing, to provide appointment reminders or information about treatment alternatives or other health-related benefits and services, in addition to other fundraising communications, that may be of interest to you. You do have the right to "opt out" with respect to receiving fundraising communications from us.

The following use and disclosures of PHI will only be made pursuant to us receiving a written authorization from you:

- Most uses and disclosure of psychotherapy notes;
- Uses and disclosure of your PHI for marketing purposes, including subsidized treatment and health care operations;
- Disclosures that constitute a sale of PHI under HIPAA; and
- Other uses and disclosures not described in this notice.

You may revoke such authorization in writing and we are required to honor and abide by that written request, except to the extent that we have already taken actions relying on your prior authorization.

You may have the following rights with respect to your PHI.

- The right to request restrictions on certain uses and disclosures of PHI, including those related to disclosures of family members, other relatives, close personal friends, or any other person identified by you. We are, however, not required to honor a request restriction except in limited circumstances which we shall explain if you ask. If we do agree to the restriction, we must abide by it unless you agree in writing to remove it.
- The right to reasonable requests to receive confidential communications of Protected Health Information by alternative means or at alternative locations.
- The right to inspect and copy your PHI.
- The right to amend your PHI.
- The right to receive an accounting of disclosures of your PHI.
- The right to obtain a paper copy of this notice from us upon request.
- The right to be advised if your unprotected PHI is intentionally or unintentionally disclosed.

If you have paid for services "out of pocket", in full and in advance, and you request that we not disclose PHI related solely to those services to a health plan, we will accommodate your request, except where we are required by law to make a disclosure.

We are required by law to maintain the privacy of your Protected Health Information and to provide you the notice of our legal duties and our privacy practice with respect to PHI.

This notice if effective as of _____ and it is our intention to abide by the terms of the Notice of Privacy Practices and HIPAA Regulations currently in effect. We reserve the right to change the terms of our Notice of Privacy Practice and to make the new notice provision effective for all PHI that we maintain. We will post and you may request a written copy of the revised Notice of Privacy Practice from our office.

You have recourse if you feel that your protections have been violated by our office. You have the right to file a formal, written complaint with office and with the Department of Health and Human Services, Office of Civil Rights. We will not retaliate against you for filing a complaint.

Feel free to contact the Practice Compliance Officer (insert name and telephone number) for more information, in person or in writing.

Exhibit 4: Receipt of Notice of Privacy Practices Written Acknowledgement Form

_____
Practice Name

I am a patient of _____. I hereby acknowledge receipt of_____'s Notice of Privacy Practices.

Name [please print]: _____

Signature: _____ Date: _____

OR

I am a parent or legal guardian of _____ [patient name]. I hereby acknowledge receipt of _____'s Notice of Privacy Practices with respect to the patient.

Name [please print]: _____

Relationship to Patient: _____ Parent_____ Legal Guardian

Signature: _____ Date: _____

Exhibit 5: Sample Privacy Policies and Procedures With Notes for Your Practice

Effective Date: _____

A. Introduction

This HIPAA Privacy Policy contains our Practice policies, procedures, and standards of conduct designed to ensure our compliance with applicable Federal laws and regulations. Failure to abide by the rules, policies and procedures established by this Policy or behavior in violation of any HIPAA law, regulation or rule may result in disciplinary action. Willful failure by any employee of the Practice to comply with the policies and procedures contained in this Plan, will result in employment dismissal. Consult the Personnel Policy Manual or contact our HIPAA Compliance Personnel if you have any questions about our Practice commitment to effective compliance routines.

B. Compliance Mission Statement

This Practice strives at all times to maintain the highest degree of integrity in its interactions with patients and the delivery of quality health care. The Practice and its employees will at all times strive to maintain compliance with all laws, rules, regulations and requirements affecting the practice of medicine and the handling of patient information. The protection of the privacy of an individual's health information and the security of an individual's electronic protected health information ("ePHI") is a critical concern to this Practice, and to the trust our patients offer in our treatment of their medical issues.

C. Privacy Policies

1. Notice of Privacy Practices

The HIPAA Privacy Regulations require health care providers to furnish patients with a written notice of the Practice's policies and procedures regarding the use and disclosure of protected health information. This Notice of Privacy Practices is the starting point under HIPAA. It describes how the Practice will be handling confidential patient information in accordance with the HIPAA regulations. Please review it carefully so that you can explain it to patients if asked.

Front desk personnel should provide each patient (new or established), at the time of the first office visit, with a copy of the Notice for review and return to the front desk prior to being seen by the doctor. The Practice will also keep on hand paper copies of the Notice for patients who ask for a take-home copy. A current copy of the Notice need only be provided once to the patient.

If the Notice is ever materially changed in terms of the description of permitted disclosures, patient rights, the Practice's legal duties, or other privacy practices, then the Notice must be redistributed to each patient.

When the patient receives the Notice, or arrives at the office for a visit after the Notice has been changed, front desk personnel should provide the patient with the Written Acknowledgement form included as Exhibit J to this Manual, and ask the patient to sign. This form merely signifies that the patient has received a copy of the Notice.

2. Staff Access to Information

HIPAA provides that staff member job functions should be reviewed to determine the level of PHI access that the staff member strictly needs to do their job. Staff members should only have the minimum access necessary, and no more.

3. Authorizations

"Authorizations" are basically patient consent forms that contain certain specific provisions required by HIPAA. Typical situations where authorizations are needed are:

- Release of medical records to qualify for life insurance coverage;
- Release of school physical results to the school, for purposes of qualifying for team sports, etc., unless the disclosure involves only immunizations and the parent or guardian has indicated their consent to the release through some other written agreement or through oral assent which has been documented. (You can also simply give the PHI directly to the parent/guardian or patient and direct them to give the information to the school);
- Clinical trial participation (release of information to pharmaceutical company is not for treatment; it's for research, which is not a HIPAA exception);
- Completion of Family Medical Leave Act forms for employers (release of information to employer is not "treatment" – easiest course again is to give the patient the information, and instruct them to give the information to the employer); or
- Psychotherapy notes in the chart (psychotherapy notes are notes by a mental health professional regarding the contents of counseling conversations and do not include such items as medication information, results of clinical tests, summary of diagnosis or symptoms or prognosis or progress to date).

When you fill out the Authorization Form, note the required "expiration date" or "expiration event." This may be any date or event desired by the patient relating to him or her or the purpose of the

disclosure. For instance, for authorization to provide the patient's employer with reports for Family and Medical Leave Act purposes, you could specify the expiration date as "termination of employment." For research disclosures only, "none" may be specified as the expiration.

Sometimes you may receive an Authorization form signed by the patient that is on "somebody else's form." For instance, frequently life insurance companies have their medical technicians obtain the patient's signature on a form at the time when all the other paperwork is filled out and the patient gives a blood sample. The life insurance company then sends the form to you, asking for the medical records. Can you accept this form, or do you need to have the patient execute the Practice's own authorization form?

You may accept an outside party's Authorization form provided it has all the elements required by HIPAA. These are:

a. A specific description of information to be used or disclosed;

b. The identification of specific individuals authorized to make the requested use or disclosure of the information;

c. The identification of specific individuals to whom the practice may make the requested use or disclosure of the information;

d. A description of each purpose of the requested use or disclosure;

e. The expiration date of the use or disclosure;

f. A statement of the patient's right to revoke the Authorization at any time in writing along with the procedure for revocation;

g. A statement that the provider may not withhold treatment if the patient refuses to sign the authorization (except as noted below for research, school physicals and other situations where treatment would not normally be provided unless the patient authorized disclosure of his or her PHI);

h. A statement that the PHI used or disclosed may be subject to re-disclosure by the party receiving the information and may no longer be protected;

i. Patient's signature and date.

If the form you are sent does not have these elements, have the patient execute the Practice's Authorization Form.

Please be sure to give the patient a copy of the authorization, when it is signed, for their records. This is required by HIPAA.

4. Minors and Incompetent Patients

As noted, minors and incompetent patients generally cannot sign the Written Acknowledgment form for themselves. Typically, they do not have the legal authority to do this. Only the person(s) who have the ability to give informed consent for the minor or incompetent patient, under state law, can exercise these rights.

Normally, in the case of a minor, it is the parent who has such right to give informed consent for the child. Therefore it is the parent who signs the Written Acknowledgment or the Authorization or other forms and who exercises the child's HIPAA rights as a patient.

5. Friends and Family

"Friends and family" pose a special challenge. These are the people who come with the patient to the doctor's office, or who pick up the phone when you call the patient's home.

Under HIPAA, friends and family, even spouses, are not entitled to the patient's PHI. Only the patient himself or herself has an absolute right to the PHI. The exception is parents of minor children or other legal guardians, who are generally to be treated for HIPAA purposes as if they were the patient, as noted above.

Having said this, HIPAA does permit some sharing of information with friends and family. HIPAA specifies that the Practice may, without written Authorization, disclose to a "family member, other relative, or a close personal friend of the [patient], or any other person identified by the [patient], the PHI directly relevant to such person's involvement with the [patient]'s care or payment related to the [patient's care]." However, there are some "strings attached." To disclose to these people (referred to in this Manual as "friends and family"), one of the following must apply:

- the Practice obtained the patient's oral or written agreement to disclosing information to the person in question;
- the Practice provided the patient with the opportunity to object to the disclosure, and the patient did not object;
- the Practice could "reasonably infer from the circumstances, based on the exercise of professional judgment, that the [patient] does not object to the disclosure," such as when the friend or family member accompanies the patient into the exam room, or when a child arrives at the doctor's office in the care of a babysitter (presumably the parent wants the babysitter to receive all resulting diagnoses and care instructions), or where a patient arrives from the nursing home in the care of a nurse's aide;
- it is an emergency situation or the patient is incapacitated, so that there is no chance to provide the patient with the opportunity to agree or object;

- the friend or family member has been sent to pick up filled prescriptions, medical supplies, x-rays, or other PHI, in which case the practice is permitted to make a reasonable inference as to the patient's best interest, in accordance with common medical practice.

If a patient wishes to identify a family member or other person with whom their medical information may be shared, the patient should be given the opportunity to designate individuals to whom it is acceptable to make a disclosure of PHI. This determination should be kept inside the patient's chart and updated as designated acceptable PHI recipients are added or dropped. It is not necessary that the patient indicate this in writing, including adding or dropping individuals from the list, since oral agreement suffices. Also, the friends and family who are named by the patient do not represent the only individuals authorized to receive the patient's PHI. As noted, there may be situations where the Practice is entitled to infer that the patient does not object to the release of information, such as in the case when the friend or family member accompanies the patient into the exam room, or a child arrives at the doctor's office in the care of a babysitter.

Simple appointment reminders can generally be left with family members even if the family member is not explicitly designated as a PHI recipient by the patient. However, check the patient's file to see if the patient has requested an alternative means of communication, and if so, honor it. In any event, do not indicate to the family member the reason for the patient's doctor visit.

6. Patient Access to Chart

Except for psychotherapy notes, patients generally have the right to inspect and obtain a copy of their medical chart. Have the patient fill out the Practice's "Request for Access to Medical Information" form. Generally, the Practice has thirty (30) days to comply with a request for access, or sixty (60) days if the information requested is not on-site.

The Practice must honor the patient's request to have the information delivered in a particular format, if this can be easily done. The Practice may be entitled to demand a copying charge.

If the patient merely wants to look at the file, not copy it, arrange a mutually convenient time and place for this to be done.

The patient's request for his or her PHI may be denied in very limited circumstances only. Access may be denied if:

- the file contains information obtained from a source other than a health care provider under a promise of confidentiality, and the access would reveal the source;

- the information requested has been compiled in a research trial that is still underway, and the patient previously agreed in writing that access would not be allowed until the trial was completed;

•a licensed health care professional has made a judgment that access would likely endanger the life or physical safety of the patient or someone else;

•the file makes reference to another person, and the licensed health professional makes a judgment that access would likely result in substantial harm to that other person;

•the information is requested by the patient's personal representative and the licensed health professional makes a judgment that access would likely result in substantial harm to the patient or another person.

If access is denied, the patient has a right to review the decision to deny access, unless it is for either of the first two reasons noted above. This review must be done by a licensed health care professional who was not involved in the original decision to deny access. Be sure to document any denials.

7. Patient Amendment of Chart

The patient has a right to request an amendment to their medical record (so long as the Practice maintains it) if he or she believes it is incorrect or incomplete. To request an amendment, the patient should complete the Practice's form "Request to Amend Medical Information". The amendment must be dated and signed by the patient.

The Practice may deny the patient's request for an amendment if it is not in writing or does not include a reason to support the request. In addition, the Practice may deny a request to amend information that:

- was not created by the Practice, unless the person or entity that created the information is no longer available to make the amendment;
- is not part of the medical information kept by or for the Practice;
- is not part of the information which the patient would be permitted to inspect and copy; or
- is accurate and complete.

The Practice must respond to the request to amend within sixty (60) days.

8. Incidental or Inadvertent Disclosures

Taken literally, HIPAA's prohibition against the disclosure of PHI would probably bring most medical practices to a standstill. For instance, the mere announcement of a patient's name in the waiting room is a disclosure of PHI – the patient's name. The same applies to sign-in sheets, overheard conversations with the check-in or check-out clerk regarding follow-up appointments, or other common situations where one patient inadvertently learns information about another patient.

Overheard conversations and other such inadvertent disclosures are called "incidental disclosures." Under HIPAA, incidental disclosures are not violations, provided that the Practice has taken reasonable steps to "safeguard" PHI and avoid incidental disclosures to the extent possible.

9. Faxes, Answering Machines, Messages, Email

As noted, HIPAA requires "reasonable safeguards" to avoid the disclosure of PHI. Although some inadvertent disclosures will be excused as "incidental," the Practice has established the following procedures to minimize the likelihood of HIPAA violations:

- Do not fax information to patients; mail it. This will minimize the chances of a fax going to the wrong fax number.

- Faxes to hospitals, other physicians, labs, and other routine recipients are acceptable. However, double check the fax number before sending, and always use a cover sheet indicating that PHI may be attached and that if the fax has gone to the wrong person, it should be returned or destroyed.

- Leaving messages on answering machines for appointment reminders is acceptable. Do not indicate the reason for the visit. Do not leave messages regarding lab or diagnostic results (even negative results) or any kind of medical information on the answering machine. Just ask that the call be returned. Do not leave a message of any kind on the answering machine if the answering machine tape does not furnish some reasonable indication that you have reached the correct number.

- Leaving messages with family members at home is also acceptable for appointment reminders. Indicate only that an appointment is scheduled, not what the visit is for. Do not leave any other kind of information, unless the Practice's records show that the person on the phone is a "friend or family" designated by the patient to be a permitted recipient of PHI.

- Leaving messages at work is very sensitive. Avoid calling the work number, but if necessary ask for a return call and nothing more.

- Appointment reminders by postcard is acceptable, so long as the appointment is of a routine nature.

Do not use email to communicate with patients unless the Privacy Officer has developed a specific written policy to control the use of this form of communication.

Exhibit 6: Patient Authorization for Practice to Release Protected Health Information

Our Notice of Privacy Practices provides information about how we may use and disclose protected health information (PHI) about you. On occasion, the patient and the Practice may want to use PHI for reasons other than treatment, payment, and health care operations, or for other purposes permitted by law. This form summarizes the anticipated use of information about you for which this authorization is required. The Practice provides this form to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Specific description of the information to be used or disclosed, including the specific purpose:

_____

_____

_____

Individuals who may use or disclose this information:

_____

_____

_____

Individuals who may receive and use the disclosed information:

_____

_____

_____

Expiration date of this authorization: _____

The above mentioned Protected Health Information may be subject to re-disclosure by the party receiving the information and may no longer be protected by the privacy rules.

continued

To the extent that this form authorizes the sale of your Protected Health Information, such a disclosure will result in remuneration to the Practice.

By signing this form, you authorize the Practice to use and disclose Protected Health Information about you for the reasons mentioned above. You have the right to revoke this authorization at any time, in writing, signed by you. However, such a revocation shall not affect any disclosures we have already made in reliance on your prior authorization. Submit your revocation to the Privacy Officer of the Practice.

This authorization was signed by: _____
Printed Name – Patient or Representative

_____ _____
Patient or Representative Signature Date

Relationship to Patient (if other than patient): _____

In front of: _____
Printed name – Practice Representative

Witness (may be Practice representative): _____
Printed name – Witness

_____ _____
Witness signature Date

Exhibit 7: Illustrations of Situations Requiring/Not Requiring Authorization

_____
Practice Name

Under the HIPAA Privacy Rule, your practice must obtain patient authorization if it wants to use PHI for non-TPO purposes.

◆ To disclose PHI about a patient to a third party (i.e., a life insurance underwriter).

◆ To market a product or services except if the marketing communication is face-to-face with the patient or it involves the provision of services of nominal value.

◆ To raise funds based on the disclosure of certain types of PHI for any entity other than your practice;

◆ For research unless your practice has a signed waiver approved by the Institutional

Review Board (IRB) for the use and disclosure of PHI or has de-identified PHI;

◆ To use psychotherapy notes, unless use or disclosure is required for:

- law enforcement purposes or legal mandates, including defending the practice in a legal action or other proceeding brought by the patient
- oversight of the provider who created the notes
- a coroner or medical examiner
- avoidance of a serious and imminent threat to health or safety;

Under the HIPAA Privacy Rule, your practice does not have to obtain patient authorization to disclose PHI

◆ To a provider who has an indirect treatment relationship with the patient;

◆ To a health oversight agency with respect to audits, civil, administrative, and/or criminal investigations, proceedings or actions, inspections, licensure or disciplinary actions;

◆ In response to a court order, court-ordered warrant, subpoena or summons;

◆ To law enforcement for the purpose of identifying or locating a suspect, fugitive, material witness or missing person, (e.g., disclosing a deceased individual's PHI if suspicion persists that death may have resulted from criminal conduct);

◆ To organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes or tissue for donation and transplantation;

◆ As required by law for public health activities and the prevention or control of disease, injury or disability, including but not limited to communicable diseases and product defects or problems (e.g., with food and dietary supplements and product labeling issues);

◆ As required by law to social or protective services with respect to victims of abuse, neglect or domestic violence;

◆ Of Armed Forces personnel for activities deemed to assure proper execution of military mission;

◆ To authorized federal officials for the conduct of lawful intelligence or counter-intelligence as authorized by the National Security Act;

◆ To authorized federal officials as it relates to protecting the President of the United

States, to foreign heads of state or other authorized persons;

◆ To the United States Department of State as it relates to obtaining security clearance, service abroad and other provisions of the Foreign Service Act;

◆ To correctional institutions or law enforcement as it relates to inmates' healthcare or the health and safety of individuals treating and transferring inmates;

◆ To a person who may have been exposed to a communicable disease, if the practice is authorized by law to notify such persons in the conduct of a public health intervention or investigation;

◆ To an employer, if the practice is a covered provider who is a member of the workforce of the employer or who provides healthcare to the patient at the request of the employer: to conduct an evaluation relating to medical surveillance of the workplace; or to evaluate whether the individual has a work-related illness or injury;

◆ To an auto insurance company or workman's compensation when they are responsible for payment of the practice's services.

Exhibit 8: Request for Limitations and Restrictions of Protected Health Information

_____
Practice Name

PATIENT PLEASE NOTE: GENERALLY, THE PRACTICE IS NOT REQUIRED TO AGREE TO YOUR REQUEST. PLEASE SEE OUR NOTICE OF PRIVACY PRACTICES FOR MORE INFORMATION REGARDING SUCH REQUESTS.

Patient Name: _____ Date of Birth:_____

Patient Address: _____
Street

_____
Apartment #

_____
City, State Zip

Type of PHI to be restricted or limited: (Please check all that apply)

❑ Home phone #
❑ Home address
❑ Occupation
❑ Name of employer
❑ Visit notes
❑ Hospital notes
❑ Prescription information
❑ Patient history
❑ Office address
❑ Office phone #
❑ Spouse's name
❑ Spouse's office phone #
❑ Other _____

How would you like your PHI restricted?

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____ _____

Signature of Patient or Legal Guardian Date

Exhibit 9: Request to Inspect and Copy Protected Health Information

_____

Practice Name

Patient Name: _____ Date of Birth:_____

Patient Address: _____
Street

_____
Apartment #

_____
City, State Zip

I understand and agree that I am financially responsible for the following fees associated with my request: copying charges, including the cost of supplies and labor, and postage related to the production of my information. I understand that the charge for this service is $_____ per page, with a minimum charge of $_____.

_____ _____
Signature of Patient or Legal Guardian Date

_____
Print Name of Patient or Legal Guardian

Exhibit 10: Patient Denial Letter

_____
Practice Name

Date:_____

Patient's Name:
Address:
Street
City, State Zip

Dear:_____

In accordance with the Final Rule for the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) issued by the U.S. Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), _____ is
Practice Name
unable to honor your request to inspect and obtain a copy of your protected health information (PHI) for the following reason(s):

[ ] _____ does not possess the information requested.
Practice Name

[ ] You have requested psychotherapy notes, as defined in the Privacy Rule, and we are not required to allow you to inspect and obtain a copy of your psychotherapy notes.

[ ] The Privacy Rule does not require the practice to permit you to inspect and obtain a copy of the requested information because it has been compiled in anticipation of, or for use in a civil, criminal or administrative action or proceeding.

[ ] The Privacy Rule does not require the practice to permit you to inspect and obtain a copy of the requested information because it is subject to or exempted by the Clinical Laboratory Improvements Amendments (CLIA) of 1988.

[ ] The Privacy Rule does not require the practice to permit you to inspect and obtain a copy of the requested information because the information was obtained from someone other than a healthcare provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

[ ] The Privacy Rule does not require the practice to permit you to inspect and obtain a copy of the requested information because the information was/is being created or obtained in the course of on-going research that includes treatment and you agreed to the denial of access when you consented to participate in the research. Your right of access will be reinstated upon the completion of the research.

[ ] The requested information is contained in records subject to the federal Privacy Act, 5 U.S.C. §552a, and this denial meets the requirements of that law.

[ ] A licensed healthcare professional has determined in his/her professional judgment that access to the requested information is reasonably likely to endanger your life or physical safety or the life or physical safety of another person.

[ ] The requested information makes reference to another person and a licensed healthcare professional has determined, in the exercise of reasonable judgment, that the requested access is reasonably likely to cause substantial harm to such other person.

[ ] You are the personal representative of the subject of the requested information, and a licensed healthcare professional has determined, in the exercise of professional judgment, that the requested information should not be provided to you.

If access to requested information has been denied for any of the last three reasons listed above, you have the right to have the denial reviewed by another licensed healthcare professional who did not participate in this denial. If you choose to have this denial reviewed, please submit a written request to our Privacy Officer at

_____ _____

Name of Privacy Officer Practice Name

_____

Address

_____ _____ _____

City State Zip Code

Our Privacy Officer will respond with a written decision within a reasonable period of time whether or not to ultimately grant or deny access to your PHI as originally requested. You may file a complaint regarding this denial with the Privacy Officer at _____ or with the Secretary of the U.S. Department of Health and Human Services. Complaints to the Secretary must be in

writing, name the Practice, describe the acts/omissions believed to violate the Privacy Rule, and be filed within 180 days of the alleged violation.

Very truly yours,

_____
Name of Practice Representative

_____
Title

If the reason for the denial is that the Practice does not maintain the PHI requested, and the Practice knows where the requested PHI is maintained, you should contact the following person or entity to obtain the requested records:

_____

_____

_____

_____

_____

Exhibit 11: Request for Correction/Amendment of Protected Health Information

_____
Practice Name

Patient Name: _____ Date of Birth:_____

Patient Address: _____
Street

_____
Apartment #

_____
City, State Zip

Type of Entry to be Amended: _____

❑ Visit note

❑ Nurse note

❑ Hospital note

❑ Prescription information

❑ Patient history

Please explain how the entry is inaccurate or incomplete.

_____

_____

_____

Please specify what the entry should say to be more accurate or complete.

_____

_____

_____

_____ _____

Signature of Patient or Legal Guardian Date

FOR INTERNAL PURPOSES ONLY:

Amendment has been: ❑ Accepted

❑ Denied

❑ Denied in part, Accepted in part

If denied (in whole or in part)*, check reason for denial:

❑ PHI was not created by this organization.

❑ PHI is not available to the patient for inspection in accordance with the law.

❑ PHI is not a part of patient's designated record set.

❑ PHI is accurate and complete.

Comments from healthcare provider who provided service:

_____

_____

_____

_____ _____

Name of Staff Member Completing Form Title

_____ _____

Signature of Healthcare Provider Who Provided Service Date

* If your request has been denied, in whole or in part, you have the right to submit a written statement disagreeing with the denial to the practice, Attn: {Name of Privacy Officer {practice address}. If you do not provide us with a statement of disagreement, you may request that we provide your original request for amendment and our denial with any future disclosures of the protected health information that is the subject of the requested amendment. Additionally, you may file a complaint with our Privacy Officer [insert name or title, and telephone number] or the Secretary of the U.S. Department of Health & Human Services.

* PRACTICE MUST INFORM PATIENT THAT A WRITTEN REQUEST IS REQUIRED, AND THAT THE PATIENT IS REQUIRED TO PROVIDE A REASON TO SUPPORT THE REQUESTED CHANGE.

Exhibit 12: Request for an Accounting of Certain Disclosures of Protected Health Information

_____
Practice Name

As a patient, you have the right to receive an accounting of certain non-routine disclosures of your identifiable health information made by our practice. Your request must state a time period prior to the date of your request (not more than 6 years). The first list you request within a 12-month period will be provided free of charge. For additional lists during the same 12-month period, you may be charged for the costs of providing the list; however the practice will notify you of the cost involved and you may choose to withdraw or modify your request.

To request an accounting of disclosures made by the practice, you must submit your request in writing to _____
Name of Privacy Officer

_____ _____
Address Phone Number

Patient Name: _____ Date of Birth:_____

Patient Address: _____
Street

_____
Apartment #

_____
City, State Zip

_____ _____
Signature of Patient or Legal Guardian Date

Exhibit 13: Sample Log to Track Disclosures of PHI

_____
Practice Name

_____
Patient Name

For each patient, you are required to keep a log of all disclosures of PHI that are (a) not made through an EHR system (such as a prescription sent via the EHR system to a pharmacy), and (b) for non-TPO reasons. (Disclosures made through an EHR system should be tracked by the system, rather than through this paper log.) For each disclosure, fill in the date it occurred along with a description of the type of disclosure. In addition, you need to provide a description of the PHI disclosed along with the names and titles to whom it was disclosed.

Date	Description of Disclosure	Description of PHI	Who Requested	To Whom PHI Was Disclosed	Approve/ Deny	Reason for Denial, Comments

Note: The practice must retain related documentation and tracking log for each patient for six (6) years from the date of its creation.

Exhibit 14: Patient Complaint Form

_____
Practice Name

Our practice values the privacy of its patients and is committed to operating our practice in a manner that promotes patient confidentiality while providing high quality patient care.

If the staff at _____ have fallen short of this goal, we want you to notify us.
Practice Name

Please be assured that your complaint will be kept confidential. Please use the space provided below to describe your complaint. It is our intent to use this feedback to better protect your rights to patient confidentiality.

_____

_____

_____

_____

_____

_____ _____
Name of Patient Date

_____ _____
Signature of Patient Phone Number

Exhibit 15: Listing of Typical Business Associates

_____
Practice Name

Note!!

Access to PHI should only be granted if these parties need access to perform services for or on behalf of your practice.

- Billing service/agency
- Collection agency
- Accountant/consultant who needs access to PHI
- Answering service
- Lockbox service
- Transcription service
- Practice management software vendor
- Electronic medical records software vendor
- Hardware maintenance service
- Off-site record storage, including cloud storage providers
- Other independent contractors who provide business/administrative services on-site

Exhibit 16: A Medical Practice Guide for the Privacy Officer to Identify Business Associates

See next page for chart

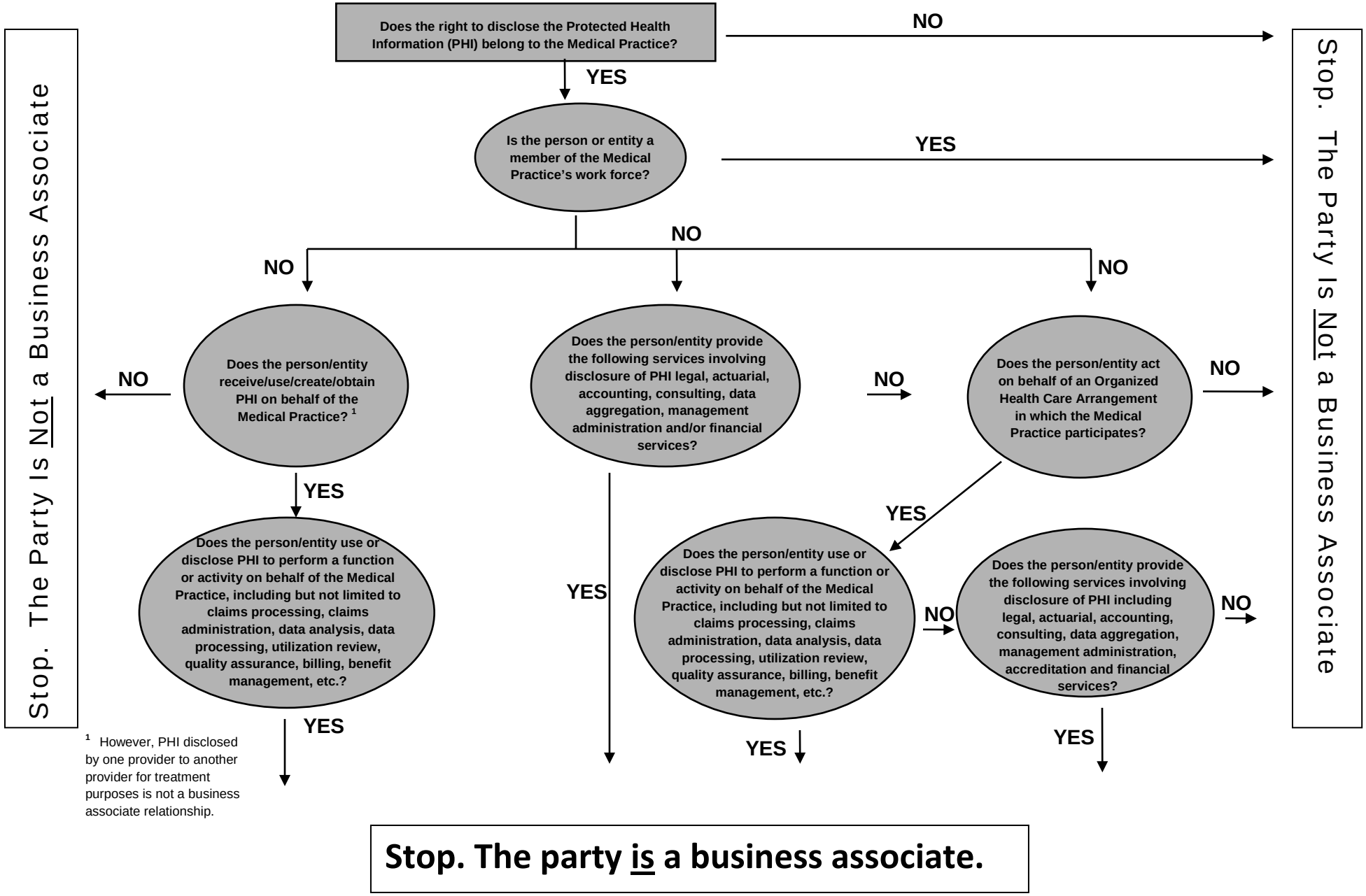

Exhibit 17: Business Associate Agreement

_____
Practice Name

* THIS DOCUMENT IS A TEMPLATE. IT DOES NOT REFLECT THE REQUIREMENTS OF STATE LAWS. YOU SHOULD CONSULT WITH ADVISORS FAMILIAR WITH YOUR STATES PRIVACY LAWS AND LAWS REGARDING THIRD PARTY BENEFICIARIES PRIOR TO USING THIS DOCUMENT.

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement, effective _____, 201_ ("Effective Date"), is entered into by and between _____ (the "Business Associate") and _____, a {physician licensed to practice medicine in the State of _____ OR a professional corporation organized under the laws of the State of _____} (the "Covered Entity") (each a "Party" and collectively the "Parties").

WHEREAS, Covered Entity and Business Associate are required to comply with the Standards for Privacy of Individually Identifiable Health Information (45 C.F.R. Parts 160 and 164, subparts A and E) ("Privacy Regulations") and for Security of electronic Protected Health Information ("PHI") (45 C.F.R. Part 164, subparts A and E ("Security Regulations"), as that term is defined in Section 164.501 of the Privacy Regulations, as promulgated by the U.S. Department of Health and Human Services ("HHS") pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), Title XIII of Division A and Title IV of Division B (the "Health Information Technology for Economic and Clinical Health" or "HITECH Act") and other applicable laws; and,

WHEREAS, the Covered Entity has engaged the Business Associate to perform "Services" as defined below; and,

WHEREAS, in the performance of the Services, the Business Associate must use and/or disclose PHI received from or transmitted to the Covered Entity; and,

WHEREAS, the Parties are committed to complying with the Privacy and Security Regulations;

NOW, THEREFORE, in consideration of the mutual promises and covenants herein contained, the Parties enter into this Business Associate Agreement ("Agreement").

1. SERVICES

Business Associate provides {billing and collection, legal, accounting, health care business consulting, or specify other type of service} services for the Covered Entity ("Services"). In the course of providing the Services, the use and disclosure of PHI between the Parties may be necessary.

2. PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION BY THE BUSINESS ASSOCIATE.

Unless otherwise specified herein and provided that such uses or disclosures are permitted under state and Federal confidentiality laws, the Business Associate may:

a. use the PHI in its possession to the extent necessary to perform the Services, subject to the limits set forth in 45 CFR §164.514 regarding limited data sets and 45 CFR §164.502(b) regarding the minimum necessary requirements;

b. disclose to its employees, subcontractors and agents the minimum amount of PHI in its possession necessary to perform the Services;

c. use or disclose PHI in its possession as directed in writing by the Covered Entity;

d. use the PHI in its possession for its proper management and administration and to fulfill any present or future legal responsibilities of the Business Associate;

e. disclose the PHI in its possession to third parties for the purpose of its proper management and administration or to fulfill any present or future legal responsibilities of the Business Associate, so long as the Business Associate represents, in writing, to the Covered Entity that (i) the disclosures are "required by law," as defined in Section 164.501 of the Privacy Regulations or (ii) the Business Associate has received written assurances from the third party regarding its confidential handling of such Protected Health Information as required in Section 164.504(e)(4) of the Privacy Regulations.

f. aggregate the PHI in its possession with the PHI of other covered entities with which the Business Associate also acts in the capacity of a business associate so long as the purpose of such aggregation is to provide the Covered Entity with data analyses relating to the Health Care Operations of the Covered Entity. Under no circumstances may the Business Associate disclose PHI of Covered Entity to another covered entity unless such disclosure is explicitly authorized herein.

g. de-identify PHI so long as the de-identification complies with Section 164.514(b) of the Privacy Regulations, and the Covered Entity maintains the documentation required by Section 164.514(b) of the Privacy Regulations, which may be in the form of a written assurance from the Business Associate. Such de-identified information is not considered PHI under the Privacy Regulations.

3. RESPONSIBILITIES OF THE BUSINESS ASSOCIATE WITH RESPECT TO PROTECTED HEALTH INFORMATION

The Business Associate further agrees to:

a. use and/or disclose the Protected Health Information only as permitted or required by this Agreement or as otherwise required by law as defined in Section 164.501 of the Privacy Regulations and as modified by HITECH;

b. use and disclose to its subcontractors, agents or other third parties, and request from the Covered Entity, only the minimum Protected Health Information necessary to perform the Services or other activities required or permitted hereunder;

c. in accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions and requirements that apply to the Business Associate with respect to such information;

d. develop appropriate internal policies and procedures to ensure compliance with this Agreement and use other reasonable efforts to maintain the security of the PHI and to prevent unauthorized use and/or disclosure of such PHI, including but not limited to, compliance with Subpart C of 45 CFR Part 164 with respect to electronic PHI;

e. to the extent the Business Associate is to carry out one or more of the Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s);

f. notify the Covered Entity's designated Privacy Officer, in writing, of any use and/or disclosure, and any other security incident of which it becomes aware, of the PHI not permitted or required hereunder within three (3) days of the Business Associate's discovery of such unauthorized use and/or disclosure or other security incident;

g. develop and implement policies and procedures for mitigating, to the greatest extent possible, any negative or unintended effects caused by the improper use and/or disclosure of PHI that the Business Associate reports to the Covered Entity;

h. make available PHI in a designated record set to the Covered Entity as necessary to satisfy the Covered Entity's obligations under 45 CFR § 164.524;

i. make any amendments to PHI in a designated record set as directed or agreed to by the Covered Entity pursuant to 45 CFR § 164.526, or take other measures as necessary to satisfy the Covered Entity's obligations under 45 CFR § 164.526;

j. provide the Covered Entity with all information the Covered Entity requests, in writing, to respond to a request by an individual for an accounting of the disclosures of the individual's PHI as permitted in Section 164.528 of the Privacy Regulations within thirty (30) days of receiving the request;

k. upon two (2) days' written notice, allow access by the Covered Entity all records, books, agreements, policies and procedures relating to the use and/or disclosure of PHI at Business Associate's offices so that the Covered Entity may determine the Business Associate's compliance with the terms of this Agreement;

l. make available all records, books, agreements, policies and procedures relating to the use and/or disclosure of PHI as requested by the Secretary of HHS for determining the Covered Entity's compliance with the Privacy and Security Regulations, subject to attorney-client and other applicable legal privileges;

m. require all of its subcontractors and agents that receive or use, or have access to, PHI to agree, in writing, to adhere to the same restrictions and conditions that apply to the Business Associate pursuant to this Agreement;

n. return to the Covered Entity or destroy, within thirty (30) days of the termination of this Agreement, the PHI in its possession and retain no copies (which for purposes of this Agreement shall mean destroy all back-up tapes); and

o. notify the Covered Entity within twenty (20) days of the discovery of any breaches of unsecured PHI as required by 45 CFR § 164.410.

4. RESPONSIBILITIES OF THE COVERED ENTITY WITH RESPECT TO PROTECTED HEALTH INFORMATION

The Covered Entity hereby agrees:

a. to advise the Business Associate, in writing, of any arrangements of the Covered Entity under the Privacy Regulations that may impact the use and/or disclosure of PHI by the Business Associate under this Agreement;

b. to provide the Business Associate with a copy of the Covered Entity's current Notice of Privacy Practices ("Notice") required by Section 164.520 of the Privacy Regulations and to of provide revised copies of the Notice, should the Notice be amended in any way;

c. to advise the Business Associate, in writing, of any revocation of any consent or authorization of any individual and of any other change in any arrangement affecting the use and or disclosure of PHI to which the Covered Entity has agreed, including, but not limited to, restrictions on use and/or disclosure of PHI pursuant to Section 164.522 of the Privacy Regulations;

d. {Use only if Services involve marketing or fundraising} to inform the Business Associate of any individual who elects to opt-out of any marketing and/or fundraising activities of the Covered Entity;

e. that Business Associate may make any use and/or disclosure of Protected Health Information as permitted in Section 164.512 with the prior written consent of the Covered Entity.

5. REPRESENTATIONS AND WARRANTIES OF BOTH PARTIES

Each Party represents and warrants to the other Party that:

a. it is duly organized, validly existing, and in good standing under the laws of the state in which it is organized or licensed;

b. it has the power to enter into this Agreement and to perform its duties and obligations hereunder;

c. all necessary corporate or other actions have been taken to authorize the execution of the Agreement and the performance of its duties and obligations;

d. neither the execution of this Agreement nor the performance of its duties and obligations hereunder will violate any provision of any other agreement, license, corporate charter or bylaws of the Party;

e. it will not enter into nor perform pursuant to any agreement that would violate or interfere with this Agreement;

f. it is not currently the subject of a voluntary or involuntary petition in bankruptcy, does not currently contemplate filing any such voluntary petition, and is not aware of any claim for the filing of an involuntary petition;

g. neither the Party, nor any of its shareholders, members, directors, officers, agents, employees or contractors have been excluded or served a notice of exclusion or have been

served with a notice of proposed exclusion, or have committed any acts which are cause for exclusion, from participation in, or had any sanctions, or civil or criminal penalties imposed under, any Federal or state healthcare program, including but not limited to Medicare or Medicaid or have been convicted, under Federal or state law of a criminal offense;

h. all of its employees, agents, representatives and contractors whose services may use or disclose PHI on behalf of that Party have been or shall be informed of the terms of this Agreement;

i. all of its employees, agents, representatives and contractors who may use or disclose PHI on behalf of that Party are under a sufficient legal duty to the respective Party, either by contract or otherwise, to enable the Party to fully comply with all provisions of this Agreement.

Each Party further agrees to notify the other Party immediately after the Party becomes aware that any of the foregoing representation and warranties may be inaccurate or may become incorrect.

6. TERM AND TERMINATION

This Agreement shall become effective on the Effective Date and shall continue unless and until either Party provides ninety (90) days' written notice of its intention to terminate the Agreement to the other, or the Agreement is otherwise terminated hereunder.

If the Covered Entity makes the determination that the Business Associate has breached a material term of this Agreement, then at the sole discretion of the Covered Entity, it may either terminate this Agreement immediately upon written notice to the Business Associate or provide the Business Associate with written notice of the material breach and allow the Business Associate fifteen (15) days to cure such breach upon mutually agreeable terms; provided, however, that if an agreement regarding a satisfactory cure is not achieved within the fifteen (15) days, the Covered Entity may immediately terminate this Agreement upon written notice to the Business Partner.

This Agreement will automatically terminate without further notice if the Business Associate no longer provides Services for the Covered Entity.

Upon termination of this Agreement for any reason, the Business Associate shall:

a. recover any PHI in the possession of its agents or contractors;

b. at the option of the Covered Entity and if feasible, either return all PHI in its possession to Covered Entity or destroy all PHI in its possession (Business Associate shall retain no copies of PHI).

If it is determined by the Business Associate that it is not feasible to return or destroy any or all of the PHI, the Business Associate must notify the Covered Entity of the specific reasons in writing. The Business Associate must continue to honor all protections, limitations and restrictions herein with

regard to the Business Associate's use and/or disclosure of PHI so retained and to limit any further uses and/or disclosures to the specific purposes that render the return or destruction of the PHI not feasible.

Further, the Business Associate shall provide written notice to the Covered Entity if it is unable, because it is not feasible, to obtain any or the entire PHI in the possession of an agent or contractor. The Business Associate shall require the agent or contractor to honor any and all protections, limitations and restrictions herein with regard to the agent's or contractor's use and/or disclosure of any PHI so retained and to limit any further uses and/or disclosures to the specific purposes that render the return or destruction of the PHI not feasible.

7. INDEMNIFICATION

The Business Associate hereby agrees to indemnify, defend and hold harmless the Covered Entity and its shareholders, directors, officers, partners, members, employees, agents and/or contractors (collectively "Indemnified Party") against any losses, liabilities, fines, penalties, costs or expenses (including reasonable attorneys' fees) which may be imposed upon the Covered Entity by reason of any suit, claim, action, proceeding or demand by any third party which results from the Business Associate's breach of this Agreement or from any negligence or wrongful acts or omissions, including failure to comply with the terms and requirements of the Privacy or Security Regulations, by the Business Associate, its shareholders, directors, officers, partners, members, employees, agents and/or contractors. This obligation of the Business Associate to indemnify the Covered Entity shall survive the termination of this Agreement for any reason.

8. GENERAL PROVISIONS

a. If the Covered Entity operates under a Joint Notice of Privacy Practices ("Joint Notice"), as defined in the Privacy Regulations, then this Agreement shall apply to all entities covered by the Joint Notice as if each such entity were the Covered Entity.

b. If the Business Associate is also a covered entity, as defined in the Privacy Regulations, then that covered entity may designate a health care component, as defined in Section 164.504 of the Privacy Regulations, which shall be considered the Business Associate hereunder.

c. This Agreement may not be modified or amended except in a writing signed by both Parties.

d. No waiver of any provision of this Agreement by either Party shall constitute a general waiver for future purposes.

e. This Agreement may not be assigned by the Business Associate without written approval of the Covered Entity. The Covered Entity may assign this Agreement upon written notice to the Business Associate.

f. This Agreement shall inure to the benefit of and be binding upon the Parties, their respective successors or assigns.

g. The invalidity or unenforceability of any particular provision of this Agreement shall not affect the other provisions hereof, and this Agreement shall be construed in all respects as though such invalid or unenforceable provision was omitted.

h. The Provisions of this Agreement shall survive termination of this Agreement to the extent necessary to effectuate their terms or indefinitely with respect to the use and disclosure of PHI.

i. Any notices to be given hereunder shall be given via U.S. Mail, return receipt requested, or by a recognized commercial express courier, as follows:

If to Business Associate, to:

_____

_____

_____

Attention: _____

Fax: ( ) _____

with a copy (which shall not constitute notice) to:

_____

_____

_____

Attention: _____

Fax: ( ) _____

If to Covered Entity, to:

_____

_____

_____

Attention: Privacy Officer

Fax: ( ) _____

with a copy (which shall not constitute notice) to:

_____

_____

_____

Attention: _____

Fax: ( ) _____

Each Party named above may change its address and/or the name of its representative by providing notice thereof in the manner provided above. If personally delivered, such notice shall be effective upon delivery. If mailed or delivered by private carrier in accordance with this Section, such notice shall be effective as of the date indicated on the return receipt whether or not such notice is accepted by the addressee.

j. This Agreement shall be construed according to the laws of the State of _____ applicable to contracts formed and wholly performed within that State. The Parties further agree that should a cause of action arise under any Federal law, the suit shall be brought in the Federal District Court where the Covered Entity is located.

k. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original. Facsimile copies hereof shall be deemed to be originals.

l. NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND OR NATURE, WHETHER SUCH LIABILITY IS ASSERTED ON THE BASIS OF CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY), OR OTHERWISE, EVEN IF THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES.

This space is intentionally left blank. The signature page follows.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be duly executed effective as of the date first stated above.

_____	_____
COVERED ENTITY	BUSINESS ASSOCIATE
By: _____	By: _____
_____	_____
Print Name:	Print Name:
_____	_____
Print Title:	Print Title:
_____	_____
Date:	Date:

Exhibit 18: Privacy Policy Training Checklist

_____
Practice Name

Training conducted on _____ by _____.
Date Name of Instructor

Attendees included those persons on the Training Documentation Form. (See Exhibit 19.) Training included: (Please check next to action item to indicate training completion.)

_____Introduction to HIPAA and the Privacy Rule

_____Introduction for Privacy Officer and Overview of Privacy Officer Responsibilities

_____Explanation of Workforce Confidentiality Agreements

_____Overview of Practice's Privacy Policies and Procedures

_____Overview of Practice's Notice of Privacy Practices

_____Explanation of Privacy Forms

_____Patient Consent Form

_____Patient Authorization Form

_____Form Requesting Restriction on Uses and Disclosures of PHI

_____Form to Inspect and Copy PHI and to Implement Access Denial

_____Form to Amend PHI

_____Form to Receive Accounting of Disclosures of PHI

_____Patient Complaint Form

_____Explanation of Who Can Disclose PHI

_____Discussion of Job Responsibilities as it Relates to PHI

_____Explanation of Minimum Necessary Standard

_____Explanation of Breach Identification/Notification Policy/Procedures

Exhibit 19: Training Documentation Form

_____
Practice Name

As a member of_____ 's workforce, I agree to adhere to the practice's policies and procedures regarding patient privacy and the security of patient protected health information (PHI). I have received a copy of the practice's policies, and have reviewed and understand these policies. I have attended the training session performed on_____.

NAME	TITLE	SIGNATURE
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Exhibit 20: Workforce Confidentiality Agreement

_____
Practice Name

I understand that _____ has a legal and ethical responsibility to
Practice Name

maintain patient privacy, including obligations to protect the confidentiality of patient information and to safeguard the privacy of patient information.

In addition, I understand that during the course of my employment/assignment/affiliation at _____, I may see or hear other Confidential Information such as
Practice Name

financial data and operational information pertaining to the practice that _____ is
Practice Name

obligated to maintain as confidential.

As a condition of my employment/assignment/affiliation with _____
Practice Name

I understand that I must sign and comply with this agreement.

By signing this document I understand and agree that:

I will disclose Patient Information and/or Confidential Information only if such disclosure complies with _____ policies, and is required for the performance of my job.
Practice Name

My personal access code(s), user ID(s), access key(s) and password(s) used to access computer systems or other equipment are to be kept confidential at all times.

I will not access or view any information other than what is required to do my job. If I have any question about whether access to certain information is required for me to do my job, I will immediately ask my supervisor for clarification.

I will not discuss any information pertaining to the practice in an area where unauthorized individuals may hear such information (for example, in hallways, on elevators, in the cafeteria, on public transportation, at restaurants, and at social events). I understand that it is not acceptable to discuss any Practice information in public areas even if specifics such as a patient's name are not used.

I will not make inquiries about any practice information for any individual or party who does not have proper authorization to access such information.

I will not make any unauthorized transmissions, copies, disclosures, inquiries, modifications, or purgings of Patient Information or Confidential Information. Such unauthorized transmissions include, but are not limited to, removing and/or transferring Patient Information or Confidential Information from _____'s computer system to unauthorized locations (for instance, home).
Practice Name

Upon termination of my employment/assignment/affiliation with _____,
Practice Name
I will immediately return all property (e.g. keys, documents, ID badges, etc.) to _____.
Practice Name

I agree that my obligations under this agreement regarding Patient Information will continue after the termination of my employment/assignment/affiliation with _____.
Practice Name

I understand that violation of this Agreement may result in disciplinary action, up to and including termination of my employment/assignment/affiliation with _____ and/or
Practice Name
suspension, restriction or loss of privileges, in accordance with _____'s policies, as
Practice Name
well as potential personal civil and criminal legal penalties.

I understand that any Confidential Information or Patient Information that I access or view at _____ does not belong to me.
Practice Name

I have read the above agreement and agree to comply with all its terms as a condition of continuing employment.

_____ _____
Signature of Employee/Physician/Student/Volunteer Date

_____
Print Your Name

Exhibit 21: Privacy Officer's Incident Event Log

_____
Practice Name

Date Received	Date Investigation Complete	Nature of Complaint	Results of Investigation	Sanctions

Exhibit 22: Breach Notification Policy

Purpose:

To provide guidance to staff when there is an acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under HIPAA which compromises the security or privacy of the Protected Health Information.

Key Terms:

Breach – the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted (under HIPAA) which compromises the security or privacy of the Protected Health Information.

Business Associate – a person or entity that uses or discloses Protected Health Information to provide a service for or on behalf of the Practice (e.g., billing companies, law firms, accounting firms). Subcontractors of the Practice's Business Associates are also deemed to be "Business Associates" under HIPAA, as are most entities that transmit or store ePHI on behalf of the Practice.

Discovered – the first day the breach is known by the practice or by exercising reasonable diligence would have been known.

Protected Health Information (PHI) – individually identifiable health information that is transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.

Unsecured PHI – any PHI which is not unusable, unreadable, or indecipherable to unauthorized individuals through the use of encryption or destruction technologies.

Workforce – employees, volunteers, trainees, and other persons of the practice is under the direct control of the practice, whether or not they are paid by the practice.

Policy:

All employees of the Practice and Business Associates are expected to secure and keep private all patient information. At no time should patient information be disclosed to another party without the authorization of the Privacy Officer. Electronic media, such as laptops, PDAs, cellular phones, blackberries, and paper files shall be secured at all times both physically and with password protections. No one is permitted to remove a patient file from the Practice for any reason unless authorized by the Privacy Officer. Employees are expected to ensure that their workstations are secure through the use of screen savers and password protection. No paper patient files shall be left unattended in any area open for viewing by the public. All employee conversations concerning patients shall be prohibited in any area open to and occupied by the public (e.g., waiting area, elevators, etc.).

It is the policy of the Practice to comply with the breach notification requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH) and the American Recovery and Reinvestment Act (ARRA). In the event of a breach of unsecured PHI, the Practice will notify all affected patients within sixty (60) days of discovery of the breach by the Practice or one of its Business Associates, in accordance with the breach notification requirements mandated by law.

Procedure:

In the event any member of the Practice workforce believes that patient information has been used or disclosed in any way that compromises the security or privacy of that information, the staff member shall immediately notify his/her supervisor or the Practice administrator. Following the discovery of a potential breach, the Practice shall initiate an investigation. The Practice's entire workforce is expected to assist management in this investigation as requested.

A risk assessment will be conducted immediately upon opening the investigation. This risk assessment shall be conducted by the Privacy Officer in accordance with HIPAA. The Privacy Officer will assess whether an exception to the breach notification rules applies or whether the result of the risk assessment indicates that not more than a low probability of compromise of the patient information exists.

Upon confirmation by the Privacy Officer that a breach has occurred, breach notification letters will be sent out to all affected individuals using the Practice's standard breach notification letter, with any appropriate modifications deemed needed by the Privacy Officer. HHS and local media outlets will be notified immediately in the event the breach affects more than 500 of the Practice's patients. If 500 or less patients are affected, the Practice will keep an accounting of the breach on the Practice breach information log, including the name and address of all affected patients contacted by the Practice and notified of the breach. This log shall be provided to the Secretary of HHS at year end. In the event of law enforcement involvement, the Practice may delay written notification of the breach, as required by law.

The breach notification letter to affected patients shall be written in plain language and must include:

1. a brief description of what happened, including the date of the breach and the date of discovery, if known;
2. a description of the types of unsecured PHI that were involved;
3. any steps the patient should take to protect himself or herself from potential harm resulting from the breach;
4. a brief description of what the Practice is doing to investigate, mitigate, and protect against future breaches; and
5. the Practice's contact information so the patient may obtain additional information if needed.

A copy of all patient correspondence shall be retained by the Practice in accordance with HIPAA (6 years) and state law record retention requirements.

Sanctions:

Practice employees who fail to comply with this policy shall be subject to disciplinary action, up to and including termination.

Exhibit 23: Breach Notification Letter

BREACH NOTIFICATION LETTER

[PRACTICE LETTERHEAD]

_____
[DATE]

Mr(s). John Smith
1234 Main Street
Anywhere, USA 00000

Dear Mr(s). Smith,

As a valued patient, we regret to inform you that our practice has discovered a (potential) breach of your personal health information. This breach was discovered on MM/DD/YYYY. We believe that information containing your (social security number, date of birth, diagnosis, name, etc.) was (stolen, inadvertently disclosed to a third party, etc.) on MM/DD/YYYY.

Because of the nature of the sensitive information breached, you may wish to contact your (credit bureaus, banks, credit card companies, other healthcare providers) and report the breach of your identifying information. As a courtesy, we have provided you with the following contact numbers:

- Equifax: 1-888-766-0008; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
- Experian: 1-888-EXPERIAN (397-3742); www.experian.com; 475 Anton Blvd., Costa Mesa, CA 92626
- TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

We recommend that you order a copy of your credit reports and continue to monitor these reports for potential fraudulent activity. You may establish a fraud alert for your accounts or a security freeze. More information about these options can be obtained from the credit bureau directly.

Please be assured that the practice is taking all steps necessary to ensure that our patient information is secure and remains private. We have recently upgraded our security standards and have (purchased encryption software, changed shredding companies, changed the locks on our doors, password protected all of our computers, etc.). We know that you expect us to keep your information safe and we can assure you we are doing everything possible to regain your trust in our practice.

Should you have any questions about the breach of your information or need additional information on what you should do as a result of the breach, please do not hesitate to contact our office at XXX-XXX-XXXX during normal business hours.

Respectfully,

_____

Mr(s). Alice/Alan Jones

_____

Practice Administrator

Exhibit 24: Breach Notification Log

The Practice Administrator will maintain a breach notification log of all breaches of unsecured PHI so as to comply with the mandatory reporting requirements under the HITECH Act. All breaches, regardless of the number of patients affected by the breach, will be recorded on this log. A copy of this log will be mailed to the Secretary of the Department of Health and Human Services on or before February 15th of each year reporting the breaches of the Practice which were discovered in the previous year.

					Notification Dates				
Control #	Date of Discovery	Date of Breach	Description of Breach	Number of Patients Involved*	Pts.	HHS	Media	Website Posting	Actions Taken/ Resolution Steps

**** All affected patients must be notified by the Practice regardless of the number of patients involved in the breach. In the event the number of patients involved exceeds 500 patients, HHS and local media sources must be notified immediately.***

Exhibit 25: APA's Position Statement on Minimum Necessary

Minimum Necessary Guidelines for Third-Party Payers for Psychiatric Treatment

The following American Psychiatric Association position statement has been developed in response to the HHS final Privacy Rule's provision that health-care "providers" (health-care professionals and facilities) disclose only the "minimum necessary" information for a given purpose. The Final Rule clarifies that "providers" may make their own determination about what is the "minimum necessary" information for a specific purpose, and also invites "professional organizations, working with their members, to assess the effects of the standards and develop policies and procedures to come into compliance with them." (p. 82472) The Rule also states that this standard is "intended to reflect and be consistent with, not override, professional judgment and standards." (p 82544)

The following guidelines are based on the cumulative professional experience of APA members with respect to current practice and the necessity of privacy for effective psychiatric care. These guidelines are based on the principle that standards for "minimum necessary" disclosure of psychiatric information to third-party payers should not exceed standards generally accepted in other medical specialties.

These guidelines address the specific delimited set of information that is necessary to process a typical claim, and therefore constitutes the minimum necessary information that may be disclosed to third party payers under the HHS Privacy Rule.

This is not a policy position about how much/what information should be documented in the record about mental-health treatment and psychotherapy. Documentation guidelines, consistent with the HHS Privacy Rule, regarding general mental-health treatment records and psychotherapy notes will be addressed in a separate document. Material in psychotherapy notes, as defined in the HIPAA Privacy Rule, is not disclosed to third-party payers.

The purpose of this document is to specify the particular items of information that the APA believes fall within the "minimum necessary" criteria for routine processing of typical insurance claims for psychiatric treatment. Psychiatrists should also familiarize themselves with applicable state statutes, which may impose additional and/or different requirements with regard to the protection of confidentiality and privacy.

The APA's guidelines for "minimum necessary" are in three parts:

1. outpatient treatment that has been authorized for payment,

2. outpatient treatment requiring pre-authorization, and

3. inpatient treatment.

#1: Outpatient treatment that has been pre-authorized for payment (including sessions that do not require any pre-authorization by payer).

The first part of the "minimum necessary" guidelines for third-party payers, which follows below, concerns outpatient treatment that has been pre-authorized for payment or outpatient treatment that is not subject to pre-authorization.

Minimum necessary information:

The following information is deemed the "minimum necessary" information that is needed by, and may therefore be disclosed to, third party payers in order for them to process a routine claim for outpatient psychiatric services that are not subject to additional pre-authorization. The guideline is based on the current HCFA 1500 claim form (attached) and the protocol for disclosures to third party payers mandated in the Washington DC and New Jersey third-party mental-health privacy statutes (attached). These statutes place explicit limits on disclosure to payers of information related to mental health treatment. The restriction on disclosure to payers in these statutes has been endorsed by the U.S. Surgeon General in his Report on Mental Health (December 1999, Chapter 7).

- Patient's name, address, date of birth, insurance information/ID number.
- Patient's diagnosis by DSM or ICD code
- Date(s), type and location of service
- Procedure code - CPT code
- Charges
- Clinician's name, ID number (i.e. SSN or EIN, and/or clinician's provider number)
- Clinician's address

If a payer cannot make a determination based on the above information, it may then request the provider to disclose additional information, limited to the following:

- Patient's status (i.e. voluntary, involuntary,
- Functional status (impairment described as none, mild, moderate or severe)
- Level of distress (described as none, mild, moderate or severe)
- Prognosis - the estimated minimum duration of the treatment for which the claim has been submitted.

#2: Outpatient treatment that requires authorization for payment.

The second part of the "minimum necessary" guidelines for third-party payers, which follows below, concerns outpatient treatment that requires authorization for payment of outpatient treatment. This includes prospective or retrospective reviews for this purpose.

Minimum necessary information:

The following information is deemed the "minimum necessary" information that is needed by, and may therefore be disclosed to, third party payers in order for them to authorize payment for outpatient psychiatric services. The guideline is based on the HCFA 1500 Claim Form, the Washington DC and NJ peer review laws, and page 1 of the APA Outpatient Treatment Report Form (12/98, attached).

Consistent with the Rule's "minimum necessary" provision, clinical information disclosed to payers for pre-authorization purposes will be used/disclosed by only those individuals who perform the review. The only information disclosed to payers' administrative personnel should be administrative billing information on the HCFA 1500 claim form.

Administrative billing information:

- Patient's name, address, date of birth, insurance information/ID number.
- Clinician's name, ID number (i.e. SSN or EIN, and/or clinician's provider number) and address
- Patient's diagnosis by DSM or ICD code - Axis I or "v" code; Axis II or III if relevant
- Date(s), type and location of service - current and planned
- Procedure code-CPT code
- Charges

Clinical information for authorization of benefits:

- Treatment planned - CPT code(s), including recommended/expected frequency
- Currently on psychiatric medications? Y/N
- Patient's status (i.e. voluntary, involuntary)
- Functional status (impairment: none, mild, moderate or severe) or Axis V (GAF)
    - Current
    - Highest in past year
    - Estimated GAF at treatment's completion (would address treatment goal)
- Level of distress (none, mild, moderate or severe) or Axis IV rating
- Prognosis - the estimated minimum duration of the treatment for which authorization is sought

#3: Minimum necessary information for inpatient psychiatric treatment.

The third part of the "minimum necessary" guidelines for third-party payers, which follows below, concerns inpatient treatment that requires authorization for payment.

Minimum necessary information:

The following information is deemed the "minimum necessary" information that is needed by, and may therefore be disclosed to, third party payers in order for them to authorize payment for inpatient psychiatric services. Consistent with the Rule's "minimum necessary" provision, clinical information disclosed to payers for pre-authorization purposes will be used/disclosed by only those individuals who perform the review. The only information disclosed to payers' administrative personnel should be administrative billing information on the HCFA 1500 claim form.

Administrative Billing Information

- Patient's name, address, date of birth, insurance information/ID number.
- Patient's diagnosis by DSM or ICD code - Axis I or "v" code; Axis II or III if relevant
- Clinician's name, ID number (i.e. SSN or EIN, and/or provider number) and address
- Date(s), type and location of service - current and planned
- Procedure code - E&M code(s) or (CPT code for ECT)
- Charges

Clinical Information for Review

- Patient's status (i.e. voluntary, involuntary)
- Functional status (impairment: none, mild, moderate or severe) or Axis V:
    - Current
    - Highest in past year
    - Estimated GAF at discharge
- Level of distress (none, mild, moderate or severe) or Axis IV:
- Current Risk Factors
    - At risk for harm to self Y/N
    - At risk for harm to others Y/N
    - Currently on psychiatric medications Y/N
    - At risk for medical complications Y/N
    - Other--specify
- Treatment planned: E&M code(s) or (CPT code for ECT), including recommended/expected frequency and duration
- Response to treatment, patient's progress, or revision in treatment plan (for authorization of additional treatment). Describe briefly:
- Inpatient treatment goal(s)
- Prognosis - the estimated minimum duration of inpatient treatment for which authorization is sought

Procedure for requesting additional information:

The preceding guidelines should be sufficient in providing the necessary information to the insurer in almost every case for the purposes previously described. In rare cases, following disclosure of the above information, if the third-party payer 1) questions the patient's entitlement to benefits, or the amount of payment requested, or 2) has reasonable cause to believe the treatment in question may be neither usual, customary or reasonable, the APA recommends the following procedure:

The disputed question/issue should be referred for an independent review by a qualified psychiatrist who is independent of the insurer, whose cost will be borne by the insurer. This reviewer will be given access to the clinical information necessary for the review. However, only the reviewer's determination, (and no additional clinical information) shall be disclosed by the treating psychiatrist or the reviewer to the insurer for this purpose. Current privacy statutes in New Jersey and the District of Columbia provide a long-standing, workable model for such a procedure.

Exhibit 26: Psychotherapy Notes Provision of the HIPAA Privacy Rule APA Resource Document

Approved by the Board of Trustees, March 2002
Approved by the Assembly, May 2001

> "The findings, opinions, and conclusions of this report do not necessarily represent the views of the officers, trustees, or all members of the American Psychiatric Association. Views expressed are those of the authors." -- *APA Operations Manual.*

This resource document was prepared by the Council on Psychiatry and the Law (submitted by the Committee on Confidentiality and revised with the Council on Psychiatry and the Law).

> The Final HIPPA Privacy Rule defines psychotherapy notes as an official record, created for use by the mental-health professional for treatment, "recorded in any medium…documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session that are **separated from the rest of the individual's medical record**..." 45 C.F.R. § 164.501 (65 Fed. Reg. at 82805) (emphasis added).
>
> The Rule does not protect psychotherapy notes when defending a malpractice suit brought by a patient or for satisfying documentation requirements of a licensing authority because it allows disclosure *without authorization* for these purposes. Save for very few other exceptions[1], "**psychotherapy notes" cannot be disclosed to anyone without the patient's specific authorization. Furthermore, such authorization *cannot* be compelled for payment, underwriting, or plan enrollment** (emphasis added).
>
> The Rule states that psychotherapy notes do ***not*** include: "medication prescription and monitoring, counseling session start and stop times, 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." 45 C.F.R. § 164.501 (65 Fed. Reg. at 82805)
> This information would be included in the patient's general treatment record, and would be available for care, payment and healthcare operations, restricted by the "minimum necessary" provision for payment and healthcare operations. [2]

Enforcement of the Final Rule will begin April 2003. The regulatory language (cited above) appears to provide strong protection for psychotherapy communications, and as HHS intended, to be consistent with the Supreme Court's reasoning in *Jaffee v. Redmond*.[3] Unfortunately, some ambiguity regarding the scope of the intended protection arises due to some imprecise language appearing in the preamble to the Rule (not in the operative text of the Rule itself) in which psychotherapy notes are incorrectly likened to narrowly defined "process notes." (Note: "process notes" is an imprecise term for which there is no universally accepted meaning; however, "process notes" are not generally used to document treatment or to be part of the official patient record[4]). The APA is concerned that the strong protection for psychotherapy

information intended by the Rule could be eroded by an unduly narrow interpretation based solely on the misleading use of the phrase "process notes" in the preamble.

Recommendation: On the basis of the profession's ethical standards, reason and experience, it is the view of the APA that the legally operative text of the Rule provides heightened privacy protection for psychotherapy notes that include some or all of the following information when documented by the treating psychiatrist, not disclosed to anyone other than the psychiatrist who created the note, and kept separately from the rest of the treatment record:

- Intimate personal content or facts
- Details of fantasies and dreams
- Process interactions
- Sensitive information about other individuals in the patient's life
- The therapist's formulations, hypotheses, or speculations
- Topics/themes discussed in therapy sessions

This kind of information is not typically needed by anyone other than the treating psychiatrist to care for the patient and is not needed for payment or health care operations. Psychotherapy notes, so defined, would serve to document and analyze the therapy and may not be used by or disclosed to persons other than the psychiatrist who created them (save for limited exceptions – see Footnote #1) without the patient's written authorization to do so. The information contained in these notes would then be afforded the higher protection provided by the Rule.

At this time, the APA suggests that members use the more inclusive definition of psychotherapy notes (delineated above) to document psychotherapy. In doing so, these notes about communication in psychotherapy, when kept separately from the rest of the record and not disclosed to anyone, would remain private under the Rule. Psychiatrists should also consider the patient's clinical state, the treatment setting, the security of the record, and relevant state law, when documenting psychotherapy.

Because the Rule's definition of psychotherapy notes is still subject to interpretation, it is possible that legal challenges will occur and the issue may ultimately be resolved in court. This resolution may come in the context of an appeal of an enforcement action involving a provider or other covered entity under the Rule. The APA is committed to advocating for the stronger, broader interpretation of the psychotherapy notes provision because it protects the privacy necessary for quality psychotherapeutic treatment and because it strongly believes that this is what the Rule was intended to accomplish.

Documentation of Psychotherapy by Psychiatrists

IV. B Documentation of Psychotherapy by Psychiatrists RESOURCE DOCUMENT

Approved by the Board of Trustees, March 2002

"The findings, opinions, and conclusions of this report do not necessarily represent the views of the officers, trustees, or all members of the American Psychiatric Association. Views expressed are those of the authors." -- *APA Operations Manual.*

Originally approved by the Board of Trustees, July 1999. Revised 2001 to integrate compliance with the Health Insurance Portability and Accountability Act (HIPAA) privacy rule promulgated in December, 2000, and effective in April, 2001, with enforcement date of April, 2003. The Commission on Psychotherapy by Psychiatrists (COPP), in consultation with the Committee on Confidentiality, has revised its Resource Document on Documentation of Psychotherapy by Psychiatrists to incorporate the requirements of the HHS Privacy Rule. The Council on Psychiatry and the Law has reviewed the paper and made some modifications acceptable to COPP.

I. Conflicting Principles and Priorities

The issues considered in the following paragraphs highlight potential conflicts between two important principles.On the one hand, medical-legal principles indicate that the medical record should be complete, factual, and accurate. On the other, the growing vulnerability of medical records necessitates great circumspection on the part of the practitioner about what to write in an official medical record lest this expose the patient to a breach of privacy and confidentiality that would undermine the psychotherapy and harm the patient. Practitioners in every individual clinical situation must be free to use their judgment in facing this dilemma. What follows is a consideration of the issues involved; it is not a standard of practice and is not binding on members of the APA.

Documentation of any medical procedure serves multiple purposes and is generally required by state statute, case law, and/or the bylaws of health care organizations. Documentation is a medical and legal record of assessment, decision-making, general management, and specific medical treatment. It should be factual, legible, and accurate. The record traditionally serves to facilitate continuity in the care of the patient by the treating psychiatrist or successors. Secondarily, with the patient's specific written, informed consent, the medical record can also be referenced to verify that services actually took place or to evaluate "medical necessity" of services rendered for purposes of claiming third-party payment. (Such usage of a detailed record of psychotherapy is, however, considered by many practitioners to be incompatible with the practice of psychotherapy.) Furthermore, the medical record may become evidence in litigation for a variety of forensic purposes, including professional liability, where documentation may make a significant difference in the exposure of the treating psychiatrist to liability (Psychiatrists' Purchasing Group, 1994).

Despite ethical standards and varying degrees of legal protection of confidentiality of the doctor-patient relationship, medical records may be open to disclosure in unanticipated ways that are beyond the control of the patient or the psychiatrist, as in the case of mandated reporting laws or other statutory exceptions to confidentiality. Such potential intrusions may present risks to the integrity of psychotherapeutic treatments. The psychiatrist should use all available legal means to protect the confidentiality of any record of psychotherapy. Psychiatric treatment, especially psychotherapy, involves sensitive, personal information about the patient and other people in the patient's life. The patient reveals this information to the psychiatrist in the faith and trust that it will be used to advance the treatment and that no information from that treatment will be revealed to any other person without informed consent for disclosure. In a landmark ruling pertaining to the admissibility of evidence in

Federal courts, the U.S. Supreme Court has explicitly acknowledged that psychotherapy requires an atmosphere of trust and confidence (Jaffee v. Redmond 116 S.Ct. 1923[1996]).

HHS protection of psychotherapy notes. This principle was further elaborated in the special protections for psychotherapy notes in the Privacy Rule promulgated by the U.S. Department of Health and Human Services (HHS) in December, 2000, in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Mandatory compliance with the rule will take effect in April, 2003. It establishes a special category of protection for psychotherapy notes, which are defined as *"notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session."* The definition excludes "medication prescription and monitoring, counseling session start and stop times, 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." (The items excluded from psychotherapy notes arecomponents of the general medical/psychiatric record.) Furthermore, "*to meet the definition of psychotherapy notes, the information must be separated from the rest of the individual's medical record.*" Notably, psychotherapy notes are still a part of the identifiable record.

Access to these notes is forbidden except with the patient's specific authorization. Authorization may not be compelled as a condition of health insurance payment or provision of services. Narrow exceptions to this protection include reporting laws (e.g., child abuse), disclosures necessary to prevent harm to the patient or others, supervision for training purposes within the ambit of confidentiality, defense against litigation by the patient, investigation by a medical examiner to determine the cause of death of the patient, health care oversight (investigation of the therapist), and disclosures authorized by the patient. The patient does not have the right to read, amend, or have a copy of psychotherapy notes. The protection continues after the death of the patient, except as noted above.

The APA believes disclosure of psychotherapy notes to third-party payers is not necessary for determining payment or medical necessity; this is consistent with the HIPAA Privacy Rule's definition of psychotherapy notes. (The reader is referred to APA Resource Document, "Psychotherapy Notes Provision of Health Insurance Portability and Accountability Act (HIPPA) Privacy Rule" (March 2002).

The rationale for special protection of psychotherapy notes is based on the deep trust needed for full disclosure of intimate personal material by a patient for the sole purpose of understanding and benefit within a psychotherapeutic relationship, delineated in *Jaffee v. Redmond*. It is keyed to the patient's expectations and the process of treatment, not to the procedure code of the service at hand. Therefore, sensitive material disclosed by a patient may be segregated in psychotherapy notes, whether the service is a specifically identified psychotherapy service (e.g., CPT 90805 to 90829, 90845, 90847) or another psychiatric service that the patient would view as establishing or including a "counseling relationship," such as psychiatric evaluation (CPT 90801) or pharmacological management defined as providing no more than a minimal amount of psychotherapy (CPT 90862). APA's resource document on Psychotherapy Notes Provision of HIPAA Privacy Rule (March 2002), developed by the Committee on Confidentiality and the Council on Psychiatry and the Law, presents a summary and clarification of the regulation insofar as it pertains to psychotherapy notes. The American Psychiatric Association is committed to seeking maximum protection of the confidentiality of psychiatric records.

The fact that it is now technically feasible to computerize medical records and transmit them electronically may present a greatly increased vulnerability to unauthorized access that may compromise confidentiality and could cause significant harm to the patient. No existing security system absolutely protects electronic records in data banks from human error or malice. Although the same risks pertain to paper records, access to electronic records may be easier to accomplish and more difficult to detect unless audit trails are maintained, accessible, and monitored. Recording psychotherapy content or process in electronic systems beyond the direct control of the practitioner (and professionals in an organized setting who are collaborating in the patient's psychotherapeutic treatment) would place a patient's private thoughts and acts at such grave risk of unauthorized disclosure as to deter or limit treatment.

Psychotherapy is a crucial part of the training of psychiatric residents. As a part of this training, residents must learn how to document psychotherapy in the medical record while maintaining confidentiality. They need to understand those instances when documentation conflicts with and potentially jeopardizes the confidentiality upon which the effectiveness of the psychotherapy is based. The same emphasis on maintaining confidentiality in documentation should also be addressed in the continuing education of practicing psychiatrists.

What follows is a suggested format, not a standard of practice, for documentation of psychotherapy by psychiatrists. It does not address issues involved in the process of releasing information to third parties, but it considers how the possibility of such release may affect documentation procedures. This discussion does not necessarily reflect current practice of documentation of psychotherapy throughout the profession. Variations occur because of state law and the requirements of individual clinical situations. The extent of documentation may vary from session to session and depends on the treatment method and intensity. A patient and/or a psychotherapist may prefer that there be no documentation, although this can pose significant liability risks to the practitioner because of the absence of contemporaneous documentation that can serve as evidence to support the standard of care provided. It should also be noted that the absence of adequate documentation makes it difficult for another psychotherapist to take over the care of a patient in cases of psychotherapist disability or death. In some states documentation is explicitly required under law.

APA's ethical principles state "Because of the sensitive and private nature of the information with which the psychiatrist deals, he/she must be circumspect in the information that he/she chooses to disclose to others about a patient." And, "Ethically the psychiatrist may disclose only that information which is relevant to a given situation. He/she should avoid offering speculation as fact." The psychiatrist should be mindful of the cautions stated in these principles when writing medical records in general, considering how likely it is that others might view the records and thus become a vehicle for disclosure. Entering any notation of psychotherapy process or content requires even greater circumspection.

II. Suggested format for documentation of psychotherapy by psychiatrists

1. ***Clinical judgment.*** The growing vulnerability of medical records necessitates great circumspection on the part of the practitioner about what to write in an official medical/psychiatric record in order not to expose the patient to a breach of privacy and confidentiality that would undermine the psychotherapy and harm the patient. Practitioners in each individual clinical situation must be free to use their judgment in coming to terms with this dilemma.

2. ***Variation in documentation procedures.*** Variations in documentation procedures may necessarily occur because of state law or the requirements of individual clinical situations. The latter may include a patient's request or the clinician's judgment that there be no identifiable documentation. Possible legal ramifications of avoiding documentation may vary in different jurisdictions.

3. ***Initial evaluation.*** The record of the patient's initial evaluation should accord with generally accepted procedures for conducting and documenting an initial psychiatric evaluation, which are beyond the scope of these recommendations. It is important that the individual clinician use judgment in regard to what information is included in the evaluation report so as not to jeopardize the patient's privacy or confidentiality. An initial evaluation may be done and documented by another psychiatrist. While documentation of the initial clinical evaluation is a part of the general medical/psychiatric record, the first meeting with a psychiatrist is the introductory experience in establishing the psychotherapy portion of psychiatric treatment. Therefore, personal information revealed by the patient during evaluation for psychotherapy may be recorded in the psychotherapy notes, subject to the definitions and exceptions that are elaborated in the HHS privacy rule.

4. ***Concise documentation of psychotherapy while respecting the privacy of the patient's mental life.*** Characteristically, the general medical/psychiatric record should concisely record only administrative material regarding the psychotherapy itself, such as the date, duration of the session, procedure code, and/or category of

psychotherapeutic intervention (e.g., psychodynamic therapy, supportive therapy, cognitive restructuring, relaxation or behavioral modification techniques, etc.). Depending on clinical judgment, the treatment setting and the security of the patient record in that particular treatment setting, some practitioners may also include a brief mention of major themes or topic(s) addressed, whereas others would consider this an unacceptable risk to the confidentiality of sensitive communications. While scheduled clock times of starting and ending the session or duration of a session may be recorded as an administrative matter if required by third parties, the Commission on Psychotherapy by Psychiatrists believes that actual times of the patient's arrival (e.g., lateness) and departure as determined by the patient (e.g., abrupt departure) are subject matter for the psychotherapy process and therefore should be recorded in the protected psychotherapy notes. If the psychiatrist were investigated for alleged fraud related to time issues, the information and the clinical explanation for the patient's deviation from the scheduled times would be available for defense in the psychotherapy notes. It is important to remember the principles of "minimum necessary" information (see following section). Clinicians should use their judgment about the information that they plan to record in the general medical/psychiatric record, especially in the context of other persons having potential access to this information.

5. ***Documentation of psychiatric management***. The general medical/psychiatric record may include other descriptive and historical information, not related to the process or content of psychotherapy, which may provide a record of responsible, diligent psychiatric management and be valuable both to patient care and to the psychiatrist in case of untoward developments. Examples of such information are:

- Clinically important objective events in the treatment setting or the patient's life (e.g., the therapist's unexpected absence, or a death in the family)
- Clinical observations of the patient's mental and physical status (e.g., noting the signs that a patient's depression has improved)
- Changes in diagnosis, DSM or ICD codes, functional status, or treatment plan (e.g., the appearance of new symptoms, return to work, new medication)
- Documentation of the psychiatrist's efforts to obtain relevant information from other sources
- Notation that a patient has been informed and indicated an understanding of the risks and benefits when medications or therapeutic procedures are changed in the course of treatment
- Collaboration with other clinicians
- Changes in the legal status of the patient (e.g., custody, guardianship, involuntary status)
- Other pertinent administrative data.

Legal reporting requirements or the need to justify hospitalization or protective intervention may necessitate documentation of information indicating danger to the patient or others, such as suicidal ideation with intention to act, child abuse, or credible threats of harm to others. The record would generally include basic management information that could enable other clinicians to coordinate effective care by a psychiatric treatment team or to maintain continuity of care if necessary. However, a responsible professional approach in today's world is to consider and justify the necessity of recording each item.

The HIPAA privacy rule mandates that disclosure of medical records information be limited to the minimum necessary to accomplish the purpose of the disclosure. The reader is referred to the APA Position Statement, Minimum Necessary Guidelines for Third-Party Payers for Psychiatric Treatment (December, 2001) when anticipating possible disclosure to third-party payers. The psychiatrist may wish to consider organizing the documentation of psychiatric management in such a way that notations of minimum necessary information can be easily extracted from the rest of the record.

6. ***Psychotherapy Notes***. Intimate personal content, details of fantasies and dreams, process interactions, sensitive information about other individuals in the patient's life, or the psychiatrist's personal reactions, hypotheses, or speculations are not necessary in a formal medical/psychiatric record. Before charting such material the clinician should carefully consider the potential vulnerability of the record to disclosure and misinterpretation. In any case, such notations, if recorded at all in identifiable form, should be confined to the protected psychotherapy notes as defined and designated by the HHS privacy rule.

7. ***Information systems considerations.*** Information entered into a computerized system that goes beyond the direct and immediate control of the treating psychiatrist (and, in an organized treatment setting, of the professionals who are collaborating in the patients care) should be stringently restricted to protect patient privacy and confidentiality. It must be limited to the minimum requirements of the system for administrative and basic clinical data and not jeopardize the essential privacy of psychotherapy material. As with any disclosure of medical records, paper or electronic, transmission of detailed clinical information to information systems outside the treatment setting must not occur without the awareness and specific, voluntary, specifically defined, written consent of the patient. Psychiatrists, along with their patients, should have the right to decide together to keep information from psychotherapy out of any computerized system. If kept on a computer, psychotherapy notes should be in a separate and secure file that is inaccessible to other users or other computers, unless the patient specifically authorizes disclosure to others.

8. ***Psychotherapy with Medical Evaluation and Management.*** The APA and the Commission on Psychotherapy by Psychiatrists affirm that psychiatrists' medical training, experience, and assessment and management skills are integral to their ongoing psychotherapeutic work. However, certain CPT codes in the 908xx series specifying "Psychotherapy with Medical Evaluation and Management (E&M)" have been interpreted by APA's experts on coding to require specific documentation that in each session thus coded the physician; 1) *assessed* the patient's condition through *history-taking and examination* and/or 2) carried out *medical decision-making* and/or 3) provided *management services*. The medical E&M service(s) may optionally be described under a separate heading from the psychotherapy service. Writing a prescription is only one of many possible actions fulfilling this requirement. Documentation mayinclude mental status or physical observations or findings, laboratory test results, prescriptions written (dates, dosages, quantities, refills, phone number of pharmacy, etc.), side effects or rationale for changes of medication, notation that a patient has been fully informed and indicated an understanding of the risks and benefits of a new medication or therapeutic procedure, compliance with medication regimen and clinical response, etc. A minimal number of E&M activities may suffice. At this time, it appears that the medical evaluation and management service (as distinct from the psychotherapy service) rendered under the "Psychotherapy with Medical E&M" codes is comparable to a Level One service under the general E&M codes (992xx) available for use by all physicians. Level One assessment could consist of one element of the mental status examination, a vital sign, or an observation of musculoskeletal status.

Documentation requirements for the general E&M (992xx) codes are still in flux. Third parties, such as Medicare, insurance companies, and HMOs are still in the process of developing policies on the kind of documentation they may require in order to reimburse patients and/or pay practitioners for CPT codes for "Psychotherapy with Medical E&M" (908xx). The APA will work hard to ensure that these new standards conform to APA recommendations for documentation of psychotherapy by psychiatrists. The contents of the psychotherapy portion of a Psychotherapy with E&M service should be documented in the protected psychotherapy notes in accordance with the principles stated above. The medical E&M portion belongs in the general medical/psychiatric record.

9. ***Consideration of patient access to records.*** Psychiatrists should be cognizant of and sensitive to the fact that patients have access to their medical records in many jurisdictions. State law may require release of the record to another physician or health care professional caring for the patient or to the patient's attorney, pursuant to valid written authorization by the patient. The HIPAA rule mandates that patients may view and submit corrections to their general medical record, but psychotherapy notes are excluded from this mandated access by the patient unless the record is involved in litigation.

10. ***Psychiatrist's personal working notes: an unresolved dilemma.*** In keeping with the APA Guidelines on Confidentiality (1987) and some authorities on psychiatry and the law (Appelbaum and Gutheil, 1991), the psychiatrist may make personal working notes, unidentified and kept physically apart from the medical record, containing intimate details of the patients mental phenomena, observations of other people in the patient's life, the psychiatrist's reflections and self-observations, hypotheses, predictions, etc. Such personal working notes are often used as a memory aid, as a guide to future work, for training, supervision or consultation, or for scientific

research that would not identify the patient. Many psychiatrists consider such uses to be crucial to the clinical care they provide. *If such notes are written, every effort should be made to exclude information that would reveal the identity of the patient to anyone but the treating psychiatrist.* If there is any risk of disclosure, patients should be informed in a general way about the use of notes for teaching and research and the ways in which identifiable disclosures will be avoided, and the patient's authorization should be obtained for such uses. As long as personal working notes are not identifiable and are not part of the patient's medical record, they are not covered by the HHS regulations.

Psychiatrists should be aware, however, that these notes might be subject to discovery during litigation, unless specifically protected by state statute. Even in protective jurisdictions the definition of personal working notes may be challenged and the notes could be subject to judicial review. It is likely that they would be considered privileged in federal judicial procedures covered by *Jaffee v. Redmond,* and in state courts that follow an approach similar to *Jaffee.* If the court does not quash the subpoena on the ground that the material is privileged, the judge would probably review it *in camera* and select what is relevant to the case at hand. *Destroying such notes after a subpoena arrives opens the psychiatrist to extreme legal risk and should never be done. Personal working notes should be destroyed as soon as their purpose has been served, and this should be done in a systematic, routine way for all cases that clearly is not designed to avoid discovery in a specific case.* Psychiatrists should acquaint themselves with prevailing law affecting personal working notes in their state. The presence or absence of notes is unrelated to the issue whether or not the psychiatrist will be required to testify.

11. ***Final clinical note***. A final clinical note at the end of treatment may summarize the psychotherapy concisely in the general medical record from a technical standpoint without divulging intimate personal information, and document the patient's status and prognosis, reasons for termination, and any recommendations made to the patient regarding further treatment and/or follow-up. It is important that the individual clinician use judgment in regard to what information is included in the final report so as not to jeopardize the patient's privacy or confidentiality.

12. ***Special situations***. Special documentation requirements established by reputable professional organizations for use by members of those organizations may apply to specified treatment methods or clinical situations. An example is The American Psychoanalytic Association's Practice Bulletin on "Charting Psychoanalysis" (American Psychoanalytic Association, 1997).

REFERENCES

American Psychiatric Association (1987). Guidelines on Confidentiality, *American Journal of Psychiatry* 144:11. Reprint available on request from the APA or at www.psych.org.

American Psychiatric Association (2001). Minimum Necessary Guidelines for Third-Party Payers for Psychiatric Treatment. Reprint available on request from the APA or at www.psych.org.

American Psychiatric Association (2002). Psychotherapy Notes Provision of HIPAA Privacy Rule. Reprint available on request from the APA or at www.psych.org.

American Psychoanalytic Association (1997). "Charting Psychoanalysis," *Journal of the American Psychoanalytic Association*, 45:656-672. Available on request from the American Psychoanalytic Association.

Appelbaum, P., and Gutheil, T. (1991). *Clinical Handbook of Psychiatry and the Law*, 2nd Ed., Williams and Wilkins.

Jaffee v. Redmond 116 S.Ct. 1923[1996]

MacBeth, JD: "Legal Issues in the Treatment of Minors." In Schetky, DH and Benedek EP*: Principles and Practice of Child and Adolescent Forensic Psychiatry*. Washington, DC: American Psychiatric Press, 2001.

Melonas, J. (1999). "Confidentiality in the Era of Managed Care," *Psychiatric Practice and Managed Care* 5(1, Jan./Feb.):6-8,12, American Psychiatric Association, Office of Healthcare Systems and Financing.

Psychiatrists' Purchasing Group, Inc. (1994). "Psychiatric Records." *In Legal and Risk Management Issues in the Practice of Psychiatry*, Chapter 7, pp. l-7.

U.S. Department of Health and Human Services. (2000). *Final Standards of Privacy for Individually Identifiable Health Information*. (Accessible at www.psych.org/pub_pol_adv/privacy122100.pdf).

Exhibit 27: Statement from the Secretary of HHS Regarding Exception to Authorization Requirement

DEPARTMENT OF HEALTH & HUMAN SERVICES Office of the Secretary

Director
Office for Civil Rights
Washington, D.C. 20201
January 15, 2013

Message to Our Nation's Health Care Providers:

In light of recent tragic and horrific events in our nation, including the mass shootings in Newtown, CT, and Aurora, CO, I wanted to take this opportunity to ensure that you are aware that the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule does not prevent your ability to disclose necessary information about a patient to law enforcement, family members of the patient, or other persons, when you believe the patient presents a serious danger to himself or other people.

The HIPAA Privacy Rule protects the privacy of patients' health information but is balanced to ensure that appropriate uses and disclosures of the information still may be made when necessary to treat a patient, to protect the nation's public health, and for other critical purposes, such as when a provider seeks to warn or report that persons may be at risk of harm because of a patient. When a health care provider believes in good faith that such a warning is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others, the Privacy Rule allows the provider,

consistent with applicable law and standards of ethical conduct, to alert those persons whom the provider believes are reasonably able to prevent or lessen the threat.

Further, the provider is presumed to have had a good faith belief when his or her belief is based upon the provider's actual knowledge (i.e., based on the provider's own interaction with the patient) or in reliance on a credible representation by a person with apparent knowledge or authority (i.e., based on a credible report from a family member of the patient or other person). These provisions may be found in the Privacy Rule at 45 CFR § 164.512(j).

Under these provisions, a health care provider may disclose patient information, including information from mental health records, if necessary, to law enforcement, family members of the patient, or any other persons who may reasonably be able to prevent or lessen the risk of harm. For example, if a mental health professional has a patient who has made a credible threat to inflict serious and imminent bodily harm on one or more persons, HIPAA permits the mental health professional to alert the police, a parent or other family member, school administrators or campus police, and others who may be able to intervene to avert harm from the threat.

In addition to professional ethical standards, most states have laws and/or court decisions which address, and in many instances require, disclosure of patient information to prevent or lessen the risk of harm. Providers should consult the laws applicable to their profession in the states where they practice, as well as 42 CFR Part 2 under federal law (governing the disclosure of substance abuse treatment records) to understand their duties and authority in situations where they have information indicating a threat to public safety.

We at the Office for Civil Rights understand that health care providers may at times have information about a patient that indicates a serious and imminent threat to health or safety. At those times, providers play an important role in protecting the safety of their patients and the broader community. I hope this letter is helpful in making clear that the HIPAA Privacy Rule does not prevent providers from sharing this information to fulfill their legal and ethical duties to warn or as otherwise necessary to prevent or lessen the risk of harm, consistent with applicable law and ethical standards.

Leon Rodriguez
Director
Office for Civil Rights

Appendix 1: Frequently Asked Questions

_____
Practice Name

Q: What is the HIPAA Privacy Rule?

A: The HIPAA Privacy Rule controls the use and disclosure of what is known as Protected Health Information (PHI). Many of the applications of the Privacy Rule are simply common sense. Others are somewhat more complex and afford the patient a great deal of flexibility in accessing the content of their medical record and how that content (PHI) is used. As well, the Privacy Rule enables the patient to control the disclosure of their PHI to certain entities.

Q: What is Protected Health Information (PHI)?

A: With few exceptions, PHI includes Individually Identifiable Health Information (IIHI) held or disclosed by a practice regardless of how it is communicated (e.g., electronically, verbally, or written).

Q: What is Individually Identifiable Information (IIHI)?

A: Any health information (including demographic information) that is collected from the patient or created or received by a healthcare provider or other covered entity or employer that relates to the past, present or future physical or mental health or condition of an individual; or the provision of healthcare; or the past, present or future payment for the provision of healthcare at your practice; and that could potentially identify an individual.

Q: What is a covered entity?

A: For purposes of the Rule, “covered entities” are health plans, health care clearinghouses and health care providers that transmit health information in electronic form as part of a transaction covered by the HIPAA electronic transaction standards. A HIPAA electronic transaction is the electronic transmission of information between two parties to carry out the financial or administrative activities related to health care, including but not limited to: health care claims or equivalent encounter information; health care payment and remittance advice; coordination of benefits; health care claim status; eligibility for a health plan; and referral certification and authorization.

Q: What is a business associate and how does a covered entity determine who their business associates are?

A: A business associate is a person or entity that is not a member of a medical practice's workforce, but who uses or discloses PHI maintained by the practice to carry out functions or activities for or on behalf of the medical practice or other covered entity. The starting point to determine who your business associates are is to examine your general ledger and see who you write checks to every month. This is usually a good indicator of who may have access to your practice's PHI.

Q: If a medical practice utilizes a locums tenens, is the practice required to execute a business associate contract with them?

A: No, for purposes of the Privacy Rule the locums tenens physician is considered to be a member of your practice's workforce and therefore required to receive the same privacy training as other providers and staff in the medical practice. The agency that placed or provided the locums tenens is not a business associate because they do not have access to PHI.

Q: When must a covered entity's staff receive training on the Privacy Rule?

A: All existing members of a covered entity's workforce are required to receive training on the Privacy Rule, both at the outset of employment and periodically thereafter It is recommended that this training be incorporated into your covered entity's new employee orientation program.

Q: When a medical practice needs to leave a message for one of its patients, how specific a message can be left on a patient's voicemail?

A: Limit the information left on a voicemail to simply the name and phone number of the person to return the phone call to. Avoid leaving lab and test results and any financial information on a voicemail.

Q: When sending mail to patients, is it acceptable to have the return address and the name of the practice on the envelope?

A: Yes, it is acceptable to still use the name and address of your practice on an envelope.

In some sensitive situations (oncology, infectious disease) you might consider the recommendation to use a post office box as a return address and remove the name of the practice in order to better protect patients' privacy; however, it remains important to ensure that information reaches patients, so such actions should be reserved for very sensitive situations. Additionally, the patient has the right to request that he/she be contacted at an alternative location (e.g., at work) or via alternative means (e.g., via telephone); therefore, if the patient is truly concerned about the manner in which he/she receives sensitive information from your practice, he/she may request a reasonable alternative. For those practices who send out appointment reminder post cards, the recommendation is that you use a fold-over postcard in order to better protect patient's confidentiality.

Q: We receive written documentation from life insurance companies requesting release of patient medical information. Our patients sign a release form that says "I authorize Doctor X to release my medical information to X Life Insurance Company." This form goes into the patient's file. Does our practice still need to get an authorization signed by the patient or can we utilize the form sent by the insurance company?

A: The form signed by the patient above does not meet HIPAA requirements. You may use the form supplied by the insurance company or patient only if contains all of the elements required by HIPAA for a valid authorization form. If not, you should require the patient to sign the practice's standard form.

The nine authorization elements required by the Privacy Rule are:

- description of the information to be used or disclosed.
- a description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization.
- name or other specific identification of the persons or class of person(s) authorized to make the requested use or disclosure.
- name or other specific identification of the person(s) or class of persons to whom the covered entity may make the requested use or disclosure.
- an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure.
- state that the information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer be protected by the Privacy Rule.
- the signature of the individual and a date.
- notify the individual that a revocation will not effect action already taken in reliance on the authorization form.
- notify the patient that a provider may not condition treatment on the patient signing the authorization form. (Please note: different rules apply if the use or disclosure is for research-related treatment or PHI created for use by a third party)
- notify the individual of the right to revoke the authorization and the process for so doing.

Q: Can you utilize a third party's authorization form or do you have to use the authorization form specific to your practice?

A: You may utilize the third party's authorization form as long as it contains the elements required by the Privacy Rule.

Q: When a medical practice is completing papers on behalf of the patient under the Family Medical Leave Act for disclosure of certain information of the Employer, are they required to get an authorization?

A: Yes, protected health information is disclosed to an employer on behalf of a patient for reasons related to Family Medical Leave Act, such as for pregnancy, an authorization signed by the patient must be obtained by the Practice prior to disclosing such information to the employer. However, no authorization is required if the disclosure to the Employer under the FMLA is required by law.

Q: When completing paperwork on behalf of a patient for disability insurance, is an authorization required prior to disclosing or returning such paperwork to the patients' employer or to the insurer?

A: If information about a patient is being disclosed to a third party such as an employer for reasons other than for treatment, payment or operations (TPO), a signed authorization

is required from the patient prior to disclosing that information. In the case of disability insurance, when disclosing information to the employer or to the disability insurer, then the practice must obtain a signed authorization from the patient.

Q: If a patient refuses to sign an authorization form, can you refuse to treat the patient?

A: In general, you cannot condition treatment upon receipt of a signed authorization form.

For example, if a medical practice presents an authorization form to a patient for signature authorizing the practice to utilize that patient's information for research purposes, and the patient refuses to sign it, the practice cannot refuse to treat the patient. However, if the patient is to receive treatment in connection with the research and he/she refuses to sign the authorization, the treatment may be denied. Also, if the treatment is requested solely for the purpose of disclosure such information to a third party (e.g., occupational drug testing), and the individual refuses to sign the authorization, the treatment may be denied.

Q: Can you convey information concerning the health and treatment of a patient to his/her spouse or immediate family?

A: Yes, you can unless the patient has explicitly indicated to the contrary or completed the "Restrictions on Uses and Disclosures of PHI" form requesting that the covered entity only communicate information to him/her and not to any family members.

Q: Do you have to document that patients have received a copy of the practice's Notice of Privacy Practices?

A: Final Privacy Rule requires covered entities to make "good faith efforts" to obtain written verification that patients have received a copy of the Notice of Privacy Practices. Covered entities should have patients sign an acknowledgement form when they receive a copy of the Notice of Privacy Practices. Medical practices should also keep a copy of this written acknowledgment in patients' medical records.

If a covered entity utilizes an electronic medical record, the patient can either sign electronically or the hard copy verification can be scanned into the patient's medical record. If a written acknowledgment from the patient cannot be obtained, the covered entity must document its efforts to receive it.

Q: If two different medical practices with separate tax identification numbers are sharing space with each other, do you need to have a signed business associate agreement between the two practices?

A: Two medical practices will not be business associates of each other merely because they share office space. However, a business associate agreement is required if one practice provides services to the other practice as a "business associate" (e.g., billing services). The business associate agreement must describe the service provided by one practice on behalf of the other and further limit the use of the PHI to the performance of such services. Remember, health care providers may disclose PHI to one another for their respective treatment and payment activities, as well as some operational activities, such as quality assurance and improvement. Of course, PHI disclosed for payment and operational purposes must be disclosed in accordance with the minimum necessary standard.

Q: If a breach of the Privacy Rule occurs and a lawsuit is filed, who would be responsible for paying the penalties? Is it the covered entity or the staff member who violated the Privacy Rule?

A: There is no private right of action under HIPAA — that is, a patient cannot bring suit against the practice for a violation of the HIPAA standards. A lawsuit filed by a third party as a result of an alleged breach of privacy or breach of patient confidentiality would be filed pursuant to particular violations of other federal or state laws, NOT HIPAA. Rather, alleged HIPAA violations would be enforced by the HHS Office for Civil Rights (the HHS department assigned with the task of enforcing HIPAA)

HIPAA violations carry fines and penalties, both civil and criminal, that would be assessed against a covered entity or an individual. However, a staff member who caused the privacy breach could (depending on the practice's own internal policies) be held accountable for any financial penalties the covered entity incurs — either by way of HIPAA violations, or private actions. (Though most practices do not have (and are not inclined to institute such penalizing policies.) Additionally, employees could be found individually liable for violations of HIPAA if acting outside of the scope of their employment.

Q: Would the staff member who caused the privacy breach be named as a defendant in a civil lawsuit filed against the practice?

A: There are particular sanctions available for use by the HHS against individuals who violate the HIPAA Privacy Rule, though the enforcement and application of those sanctions will depend upon the enforcement decision made by the Office for Civil Rights.

As noted above, HIPAA does not create a private right of action against individuals. If the practice were sued by an individual as a result of a breach of state or other federal confidentiality or privacy duties, it would not be unusual for the plaintiff to name individuals, as well as the practice, in such a suit.

Medical practices and other covered entities should take extra care in training their staff to make sure they understand the importance of patient privacy. Additionally, physicians and staff should be trained

annually and should be required to sign workforce confidentiality agreements which will indicate the types of sanctions that may be applied to the employee (physician or staff, if applicable) who intentionally or unintentionally causes the practice to fail to meet its obligations under the Privacy Rule.

Q: Are Workforce Confidentiality Agreements required by HIPAA?

A: No, they are not required by HIPAA. It is a recommendation that practices consider using them in order to stress to employees the importance of HIPAA compliance, with the goal of preventing privacy breaches.

Q: Are medical residents considered to be Business Associates of the medical practice?

A: No, medical residents are acting as part of the medical practice's workforce and therefore should receive privacy training just as any other physician or staff member would.

In addition, medical residents should sign workforce confidentiality agreements.

Q: If a medical practice has information in a patient's medical record that was acquired from another medical provider, is the medical practice required to release that information when it receives a request from a third party?

A: If you receive a patient's authorization to release all of his/her medical records (i.e., the patient has not placed any restrictions on what you are to release to the third party), you should release that set of medical and billing records maintained by the practice and which are used in whole or in part to make decisions about the individual — in essence, the entire medical record created by your practice and any medical record received by the practice (relating to the patient) from other providers.

Q: Do medical practices need a business associate agreement with their janitor or cleaning service?

A: Business associate agreements are only required for third parties who are not employees of the medical practice but who provide a function on behalf of the practice that requires the use of patients' PHI. Cleaning personnel do not need to have access to PHI in order to clean the medical practice. Practices must implement administrative, technical and physical safeguards to protect PHI; therefore, the practice's policies should work to prevent such exposures (e.g., appropriate document destruction, locked file cabinets, etc.)

Q: Does a covered entity need a business associate agreement with a third party's employees or the third party (e.g., a vendor)?

A: The covered entity should enter into a business associate agreement with the company (e.g., a vendor) and not the company's employees. For example, if a medical practice engages a consulting firm to conduct a coding audit in your medical practice, the medical practice would enter into a business associate agreement with the consulting firm and not with the individual consultants who will be onsite conducting the coding audit.

Q: Does the "Amend PHI" form need to be completed by the patient when there is a change in a patient's demographic information?

A: No, the medical practice can simply update the demographic information as given by the patient either verbally or in written form. The "Amend PHI" form should be used by covered entities when a patient requests that medical information in his/her medical record be changed or deleted.

Q: If a medical practice has a new patient on its schedule who has first been seen in the local hospital, is the medical practice allowed to request information from the hospital in advance of seeing the patient?

A: Yes, HIPAA does not preclude covered entities who are health care providers from sharing patient PHI with each other for treatment or payment purposes.

Q: If a patient wants a copy of his/her medical record, is the medical practice allowed to charge the patient for it?

A: Laws surrounding the copying of medical records vary from state to state. It is recommended that a practice check its state law before charging patients for copying their medical records. Your state medical association may be able to provide you with information in this regard.

Appendix 2: HIPAA Resources

_____
Practice Name

Centers for Medicare and Medicaid Services
http://www.cms.gov

Office for Civil Rights
http://www.hhs.gov/ocr/privacy/

U.S. Department of Health and Human Services
http://www.hhs.gov

Appendix 3: Facsimile Transmittal

_____
Practice Name

Facsimile Transmittal

To:_____ Fax:_____

From: _____ Date:_____

Re: _____ Pages:_____

CC:_____

❑ Urgent ❑ For Review ❑ Please Comment ❑ Please Reply ❑ Please Recycle

_____

Notes: Note: The information contained in this facsimile may be privileged and confidential and protected from disclosure. If the reader of this facsimile is not the intended recipient, you are hereby notified that any reading, dissemination, distribution, copying, or other use of this facsimile is strictly prohibited. If you have received this facsimile in error, please notify the sender immediately by telephone at and destroy this facsimile. Thank you.

Appendix 4: Forms Checklist

_____
Practice Name

List of materials to be given to each patient:

1. Notice of Privacy Practices (including a written acknowledgment form)

List of materials/forms to have available upon patient request:

1. Notice of Privacy Practices
2. Patient Authorization for Use and Disclosure of Protected Health Information to Third Parties
3. Request for Limitations and Restrictions of Protected Health Information
4. Request to Inspect and Copy Protected Health Information
5. Request for Correction/Amendment of Protected Health Information
6. Request for an Accounting of Certain Disclosures of Protected Health Information
7. Patient Complaint Form

Appendix 5: Patient Consent Form

_____
Practice Name

See Appendix 6 for the Patient Consent for Use and Disclosure of Protected Health Information.

A PATIENT CONSENT FOR THE USE AND DISCLOSURE OF PHI FOR TPO IS OPTIONAL AND IS NOT REQUIRED BY THE PRIVACY RULE. However, you may wish to obtain or continue to obtain patient consent to use PHI for TPO purposes. (Consult with your practice's legal counsel.) Medical practices should be cautioned that a Consent may not take the place of an authorization required under the Privacy Rule. Also, a Consent may be bundled with the patient's acknowledgment of the Notice of Privacy Practices. NOTE: If you voluntarily choose to use a consent form, your state law may have consent requirements with which your practice must comply.

(OPTIONAL)
• Fill in Practice Name on Exhibit 6.

• Photocopy and make available the Patient Consent Form for all patients at each facility in which your practice operates.

Note:

• The Notice of Privacy Practices may inform patients of this option.

• At registration of new patients and for established patients who have not executed this form, the practice front office staff may provide this form to its patients for completion.

• Patient completes, signs and dates the Patient Consent Form; staff reviews it for accuracy and files it in the patient's chart.

• Document and retain the Consent for six (6) years (at a minimum) after the patient's relationship with the practice ends. If the Consent is a part of the medical record, then the practice must retain it for as long as state law requires your medical records to be retained.

• If patient revokes the consent, this revocation must be included in patient's record.

continued

• WARNING: Upon the revocation of a patient's Consent, the practice may no longer use or disclose his/her PHI for TPO; however, the practice may continue to use any PHI obtained or created up to the date of revocation for TPO purposes.

• A Consent is OPTIONAL — a practice may not require a patient to sign a consent prior to the delivery of care.

• A Consent does not take the place of an authorization.

• Practices who decide to obtain signed consent forms from its patients must still make a good faith effort to obtain written acknowledgement from them of receipt of the Notice of Privacy Practices in order to be in compliance with the Privacy Rule.

• Obtaining patient consent forms is optional and not required by the Privacy Rule.

Appendix 6: Patient Consent for Use and Disclosure of Protected Health Information (OPTIONAL)

_____
Practice Name

Note!!
Utilization of this form is OPTIONAL AND NOT REQUIRED under the Privacy Rule. This form may not meet your state's requirements, so consult with your legal counsel before using the form in your practice.

I hereby give my consent for _____ to use and disclose protected
Practice Name
health information (PHI) about me to carry out treatment, payment and healthcare operations (TPO). (_____'s Notice of Privacy Practices provides a more complete
Practice Name
description of such uses and disclosures.)

I have the right to review the Notice of Privacy Practices prior to signing this consent.
_____ reserves the right to revise its Notice of Privacy Practices at anytime.
Practice Name
A revised Notice of Privacy Practices may be obtained by forwarding a written request to
_____ Privacy Officer at _____.
Practice Name [Street Address, City, State Zip]

With this consent, _____ may call my home or other alternative
Practice Name
location and leave a message on voice mail or in person in reference to any items that assist the practice in carrying out TPO, such as appointment reminders, insurance items and any calls pertaining to my clinical care, including laboratory results among others.

With this consent, _____ may mail to my home or other alternative
Practice Name
location any items that assist the practice in carrying out TPO, such as appointment reminder cards and patient statements as long as they are marked Personal and Confidential.

With this consent, _____ may e-mail to my home or other alternative
Practice Name
location any items that assist the practice in carrying out TPO, such as appointment reminder cards and patient statements. I have the right to request that _____
Practice Name
restrict how it uses or discloses my PHI to carry out TPO. However, the practice is not required to agree to my requested restrictions, but if it does, it is bound by this agreement.

By signing this form, I am consenting to _____'s use and disclosure of
Practice Name
my PHI to carry out TPO.

I may revoke my consent in writing except to the extent that the practice has already made disclosures in reliance upon my prior consent. If I do not sign this consent, or later revoke it, _____ may decline to provide treatment to me.
Practice Name

_____
Signature of Patient or Legal Guardian

_____ _____
Patient's Name Date

_____
Print Name of Patient or Legal Guardian

Appendix 7: Determine Whether Your Practice Uses and Discloses PHI for Research Purposes

_____
Practice Name

If your practice does not use PHI for research purposes, skip to APPENDIX 9.

Practices may use a patient's PHI for research purposes under the following conditions: (1) the practice obtains signed authorization from the patient; (2) an Institutional Review Board (IRB) or Privacy Board grants a waiver of authorization for the research; or (3) the Practice limits the disclosure of PHI to conform with the Limited Data Set rules and obtains Data Use Agreements, as necessary.

Research Authorizations

If the Practice does not qualify or obtain a research authorization waiver from an IRB or Privacy Board, the Practice must obtain an authorization from the patient prior to using or disclosing his/her PHI for research purposes.

See Step 8 for the list of required elements to all authorizations. Please note that "none" may be used as the expiration date/event on the authorization, as long as it includes a corresponding statement that the authorization will have no expiration date or event. As with other authorizations, the research authorization must clearly indicate that the patient may revoke the authorization and must provide the procedure for doing the same. If an individual revokes his/her authorization for research, the PHI used or disclosed prior to such revocation may continue to be used to the extent necessary to preserve the integrity of the research study. However, after such revocation, the practice may not continue to use or disclose additional PHI.

Exhibit 6 may be used to obtain authorization from the patient to use and disclose PHI for research purposes.

If the research also involves the provision of research-related treatment to the individual and the individual refuses to sign an authorization for the research, than the practice may withhold such research-related treatment.

Research Waiver

In lieu of a patient authorization, PHI may be used or disclosed for research purposes in limited instances based upon IRB or Privacy Board determinations that PHI will remain protected and that the research project depends upon such PHI. The IRB or Privacy Board may waive all or part of the requirement to obtain a patient authorization, if the following criteria are satisfied:

◆ the use or disclosure of PHI involves no more than minimal risk to the privacy of the individual, based on at least the following:

- a plan to protect the PHI from improper use and disclosure;
- a plan to destroy the PHI at the earliest opportunity unless retention of the PHI is required by law; and
- a written assurance that the PHI will not be used or disclosed to a third party except as required by law or permitted by an authorization.

◆ the research cannot be conducted without a waiver of authorization; and

◆ the research cannot be conducted without access to the patient's PHI.

Current/Ongoing Research Protocols

If the practice is currently using or disclosing PHI in accordance with existing research protocols, the practice may continue to do so provided that the practice has received one of the following unrestricted permissions:

◆ written authorization or other express legal permission from an individual to use or disclose PHI for the research;

◆ the informed consent of the individual to participate in the research; or

◆ a waiver by an IRB of the informed consent, in accordance with applicable law, so long as informed consent is not subsequently sought from individuals participating in the research.

Note:

• Treatment of a patient may be conditioned on completion of the authorization form if the treatment is being provided solely for the purposes of research. If not, then the practice cannot condition treatment based on receiving a signed authorization form.

• Once the authorization is signed, the practice is required to provide a copy of the signed authorization to the patient. In addition, the practice must retain a record of the authorization for six (6) years at a minimum.

continued

• If the practice will receive any payment from a third party for using and disclosing the patient's PHI for research purposes, then the authorization form must include a statement to that effect.

• Since IRBs and Privacy Boards may have difficulty in interpreting data sent by practices and because their review may be purely objective, HHS intends to issue further guidance to address these concerns.

Limited Data Set

If the Practice intends to use or disclose patient PHI for the creation of a Limited Data Set to be used for research purposes, then the Practice should enter into Data Use Agreement(s) (and/or Business Associate Agreements, with appropriate language included regarding Limited Data Set use) with the recipients of the Limited Data Set, as described in Appendix 8.

Appendix 8: Implement a Data Use Agreement

_____
Practice Name

HHS allows practices to create a Limited Data Set for certain limited purposes including: research, public health and health care operations. The Limited Data Set may include the following identifiable information: admission, discharge and service dates; date of death; age (including age 90 or over); and geographic subdivision, including town or city, state or five-digit zip codes. If a practice uses and/or discloses information in a Limited Data Set, then written patient authorizations and IRB/Privacy Board waivers are not needed. For example, a practice may create a Limited Data Set to disclose public health information not already permitted under HIPAA, such as reporting to privately sponsored disease register.

If Limited Data Sets are to be used, the practice must implement a Data Use Agreement with the person(s) or entity conducting the research, public health and/or health care organizations. The Privacy Rule does not mandate a specific format for the Data Use Agreement, so practices have the flexibility to use a format that best suits their purposes. However, the Data Use Agreement must state the following:

- the permitted uses and disclosures of the Limited Data Set;
- who can use or receive the data; and
- that the recipients of the data must not:
    - re-identify the data or contact the individuals;
    - use or disclose the information except as permitted by the agreement or by law;
    - use appropriate safeguards to prevent unauthorized use or disclosure;
    - report to the practice any unauthorized uses or disclosures; and
    - ensure that its agents and subcontractors agree to the same restrictions and conditions.

If the practice conducts in-house research and the researcher is an employee of the practice, then the requirements of the Data Use Agreement could be met by having the employee sign a workforce confidentiality agreement. Other agreement formats can be used, so long as they contain the requisite language. In addition, Data Use Agreements can be combined with a Business Associate Agreement to form a single agreement.

Appendix 9: Determine Whether Your Practice Participates in an Organized Health Care Arrangement (OHCA)

_____
Practice Name

An organized health care arrangement (OHCA) means one of two things for medical practices:

1. a clinically integrated care setting where patients receive treatment from more than one health care provider; or

2. an organized system of healthcare where more than one covered entity participates, and in which the participating covered entities:

- inform the public that they are participating in a joint arrangement; and,

- where they participated in at least one of the following joint activities: utilization review, quality assessment and improvement activities, or payment activities that involve shared risk.

Typical examples of organized health care arrangements for medical practices include:

- A hospital and its medical staff members;

- An independent practice association that includes a number of physicians operating their practices autonomously, but participating in quality assurance and/or shared risk payment activities.

HIPAA provides OHCAs some flexibility under which to apply the Privacy Rule's requirements so that the OHCA can best suit the structure of their businesses. OHCA participants may disclose PHI to one another for the TPO activities of the OHCA.

If practice physicians participate in an OHCA as medical staff members, then those physicians should not be required to provide patients with a Notice of Privacy Practices while practicing in the hospital. The hospital will likely provide patients with the Notice as part of the admissions process and obtain the required acknowledgement. Practices may want to confirm that procedure with the hospital.

Regarding a physician's obligation to inform the public that he/she is participating in a joint arrangement, the actual Notice of Privacy Practices of the OHCA ideally would disclose such information to the patient so that each individual physician does not have to self-disclose. If a physician chooses not

to become part of an OHCA and provides services to patients, then those physicians must provide a Notice of Privacy Practices to their patients and obtain a signed acknowledgement from the patient.

• You may only develop a joint Notice of Privacy Practices if your organization qualifies as an OHCA, together with another participating covered entity. If it does not qualify, then your practice must develop its own Notice of Privacy Practices.

• Just because your practice shares space with another practice, does not automatically mean that the two practices are operating as an OHCA. See the requirements of an OHCA, above.

• If you maintain a web site for the OHCA, you must post the Joint Notice of Privacy Practices on the web site.