HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

SECURITY STANDARDS

A Guide for Physician Practices

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 security laws will continue to apply following the compliance date of the HIPAA security 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 the American Psychiatric Association, American Academy of Dermatology Association, Health Care Law Associates, P.C,. 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) Security 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.

HEALTH CARE LAW ASSOCIATES, P.C, AMERICAN PSYCHIATRIC ASSOCIATION AND THE 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.

The American Psychiatric Association and the American Academy of Dermatology Association are technology/vendor neutral companies. The use of trademarked names within this manual is for reference purposes only and should not be considered as a form of endorsement.

Developed by: American Psychiatric Association www.psychiatry.org and American Academy of Dermatology Association

Legal Guidance provided by: Health Care Law Associates, P.C. www.thehealthcaregroup.com

Contents

Introduction to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule 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 individual's personal healthcare information. HIPAA evolved and was passed, in part, to improve the efficiency and effectiveness of the healthcare system by standardizing the transmission of certain administrative and financial information and by protecting the privacy and security of personal health information. 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").

On December 29, 2000 and on August 14, 2002, HHS published the final Standards for Privacy of Individually Identifiable Health Information (Privacy Rule); the Privacy Rule underwent substantial changes as a result of HITECH and its various implementing regulations. The Privacy Rule established mandatory guidelines regarding the use and disclosure of protected health information.

See the American Psychiatric Association's Privacy Manual for additional details about the Privacy Rule and Compliance Guidelines.

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 greater knowledge of the content of their medical record and how that content (PHI) is used. Also, the Privacy Rule enables the patient to control the disclosure of their PHI to certain entities.

Prior to the Security Rule, there had been no national or consistent industry standard governing the security of an individual's health information. The Security Rule focuses on requirements for covered entities (including medical practices) to protect and safeguard the confidentiality of PHI created, maintained, and transmitted in electronic form. The purpose of the Security Rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (EPHI). Among other things, the practice's computer network, access to the network, and the method by which the practice stores and handles such data come under close scrutiny by the Security Rule.

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

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

The Security Rule requires covered entities to implement basic safeguards to protect EPHI from unauthorized access, alteration, deletion, and transmission. Accordingly, the Rule is broadly written and the detail and means of actual application among parties will vary, though all must meet the standards set forth in the Rule. Unlike the Privacy Rule, the Security Rule is much more flexible and gives practices much more leeway in how to comply with the Rule. The Security Rule was written to be scalable among covered entities of various forms, sizes, and technological sophistication. This manual includes detailed checklists, "how-to" guides, and sample documents to facilitate your practice's efforts to comply with the Security Rule. The Security Rule is comprised of three primary security safeguards: administrative safeguards, physical safeguards, and technical safeguards. Within each of these three safeguards, there are a number of specific security standards that must be satisfied by the practice. The security standards are intended to support the protection of the electronic health information covered by the Privacy Rule. See Exhibit 2 for a matrix of the multiple components of the Security Rule. Compliance with each of the elements of the Rule is necessary.

However, for certain standards, the Rule requires a particular means of compliance– referred to as the **necessary** implementation specifications. For other standards, the Rule requires that the practice address whether the implementation specifications are applicable and reasonable before the practice is required to implement the specifications set forth in the Rule or take other specific action – referred to as the **addressable** implementation specifications. This manual will walk your practice through each element of the Rule and assist you in satisfying each of its implementation specifications – whether they are required or addressable.

How to Use this Manual

The Overview and the Glossary can be copied for use within your practice without specific permission and shared with all staff and physicians as a training tool.

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

The "Snapshot Compliance Component" with each step provides an overview of the safeguard(s), standard(s), and implementation specifications that apply. Practices will quickly be able to determine which implementation specifications are either **required** or **addressable**.

The "To Do" box on each page provides suggestions for meeting the Security Rule requirements.

The "Note" box provides cautions, observations, and recommendations that will further guide your practice to HIPAA compliance. Items contained within the "Note" box are not required by the Security Rule, but your practice may find them helpful in the implementation of the Security Rule's required elements.

The Internal Security Checklist provides useful, practical insight into the Security Rule and the more general security 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 the Security Rule in your practice.

Please note that your Security Official or a designated staff member will need to fill in your practice's name on each Exhibit if you wish to convert this manual into your practice's security compliance plan and record.

Appendix 1 is a flow chart to help practices determine what steps need to be taken in order to satisfy an **addressable** implementation specification.

Appendix 3 lists web sites that contain useful information pertaining to HIPAA.

Planning Tips:

- Budget: Practices may need to prepare a budget for implementing the HIPAA Security Standard. Some expenses may be incurred depending on the necessary measures put into place. These expenses will vary.
- Protective Software: A quick search of your local office supply store or software vendor will provide practices with many of the protective software packages needed to comply with the HIPAA Security Rule.
- Backup software
- Recovery software
- Drive copy software
- Virus scanning software
- Firewall software
- Cleaning software
- Security and Intrusion protection software
- Combinations of all the above

This manual should be used in conjunction with the Privacy Manual or your practice's other Privacy Rule compliance plan(s).

Except for the Overview and Glossary, this manual does NOT include such items as training materials, specific practice procedures, or state specific information/requirements.

A HIPAA Glossary

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

Access
The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource that creates, maintains, or transmits EPHI.

Access Authorization
Process by which rules are established for granting and/or restricting access to a user, terminal/workstation, transaction, program, or process for the purpose of creating, maintaining, or transmitting EPHI. For example, the billing staff usually only needs access to the current visit notes, not the entire clinical record.

Access Control
A method of restricting access to resources; allowing only privileged entities access. Types of access control include mandatory access control, discretionary access control, time-of-day, classification. For example, passwords can provide a certain level of access control.

Addressable Specification
One of two types of implementation specifications addressed by the Security Rule. A covered entity must implement IF it is reasonable and appropriate OR, if not, either document why it's not reasonable and appropriate AND implement an "equivalent alternative measure if reasonable and appropriate." (See also Required Specification.)

Administrative Safeguards
Formal documented practices to protect EPHI. This includes the selection and execution of security measures and the management of personnel as it relates to protecting EPHI.

Audit Trail
Data collected and potentially used to facilitate a security audit to include the who (login ID), what (read-only, modify, delete, add, etc.), and when (date/time stamp).

Audit Controls
Mechanisms employed to record and examine system activity.

Authentication
The confirmation that a person is the one he/she claims to be. Authentication processes or mechanisms are those that are utilized to verify the identity of a person (see Password).

Automatic Logoffs
A process that a computer server uses to disconnect a connection to the computer server when no data has been transmitted for a given period of time.

Biometric Identification
Identification system that identifies a human with measurement of a physical feature of the individual. (e.g., hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, and hand written signature).

Breach

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

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

Confidentiality
The process by which data or information is not made available or disclosed to unauthorized persons or processes.

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.

Criticality
Addresses those assets that are critical to the function of a practice and expresses the significance given to a functional failure of those important assets.

Cryptographic Key
A special type of password created by a computer outfitted with encryption technology, that when used, will secure data (encrypt) being transmitted over a network or the Internet. The receiving computer of the data must also know the password in order to display the secured data (decrypt). There are two types of cryptographic keys, private (symmetric) and public (asymmetric). Once the encryption software is loaded, the cryptographic key is part of the practice's computer system. When e-mail is sent, the "key" performs its function without any extra effort on the part of the person sending the e-mail.

Cryptography
The study of encoding (putting message into a code) and decoding (converting a message from a code into plain text).

Decryption
Decoding data that has been encrypted into a secret format. Decrypting encrypted messages requires a secret key or password. (See Encryption)

Department of Health and Human Services (DHHS)
A department of the executive branch of the federal government that has overall responsibility for implementing HIPAA.

Direct Treatment Relationship
A treatment relationship between the 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.)

Disaster Recovery
Process whereby a practice would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.

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

Electronic Protected Health Information (EPHI)
Protected health information (PHI) transmitted by electronic media or maintained by electronic media.

Electronic Media

- Electronic Storage Medium including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card (e.g., CD, DVD, tape, etc.).

- Transmission Medium used to exchange information already in electronic storage media. Transmission media includes the following: the Internet (wide-open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, virtual private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions of paper, via facsimile, or voice, via telephone, are not considered to be transmission via electronic media because the information being exchanged did not exist in electronic form before the transmission, with the exception of computerized fax capabilities).

Emergency Mode Operation
Procedures that enable a covered entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure.

Encryption
The use of a computer entered formula to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key.

Facility Security Plan
Plan to safeguard the premises and building(s) (exterior and interior) of a covered entity from unauthorized physical access and to safeguard the equipment therein from unauthorized physical access, tampering, and theft.

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 (DHHS) 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 Clearinghouse
Under HIPAA, this is a covered 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 a 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 the use of EPHI 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.

Identification
The process that enables a computer system to recognize a computer user. The most common form of identification is a User ID.

Implementation Specification
Specific requirements or instructions for implementing a standard. Specifications are designated as either required or addressable per the Security Rule (e.g., Covered entities are required to perform a security risk assessment. Covered entities must address the necessity of implementing facility access controls.)

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

- The healthcare indirect provider typically provides healthcare services or products and then reports the diagnosis or results to a direct healthcare provider who uses this information to provide care 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.

Information System
A computer system including a desktop, laptop, or a PDA loaded with software that maintains data.

Integrity
The trait that data or information have not been altered or destroyed in an unauthorized manner.

Internal Audits
The in-house review of the records of system activity (for example, logins, file accesses, security incidents) maintained by an organization.

IT
Information technology or information technologist.

Malicious Software
Software designed to damage or disrupt a system (e.g., virus).

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.

Need-To-Know
A security principle stating that a user should have access only to the data he or she needs to perform a particular function. Per the Security Standard, this must be addressed within the workforce job description.

Office of Civil Rights (OCR)
The HHS sub-department responsible for the enforcement of the HIPAA Privacy and Security Rules.

Operations
See Healthcare Operations.

Organized Health Care Arrangement (OHCA)
A clinically integrated healthcare setting in which individuals typically receive healthcare from more than one provider, or an organized system of healthcare in which more than one covered entity participates and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement, and participate in a joint arrangement that includes at least one of the following:

- Utilization review;
- Quality assessment and improvement activities; or
- Payment activities.

Password
A confidential numeric and/or character string used in conjunction with a user ID to verify the identity of the individual attempting to gain access to a computer system (see Authentication).

Payer
In healthcare, an entity that assumes the risk of paying for medical treatments. This can be a self-pay 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 Identification Number (PIN)
A number or code assigned to an individual used to provide verification of identity.

Physical Safeguards
Procedures to protect computer systems, buildings, and other equipment from fire and other natural and environmental hazards, as well as intrusion.

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).

Required Specification
An implementation specification that a covered entity is required to implement based on the Security Rule (e.g., covered entities are required to perform a security risk assessment).

Scalable
Capable of being scaled. The HIPAA Security Rule is scalable to the needs of the individual practices (see Addressable Specification).

Screensaver
A screensaver is a computer file that was originally designed to protect a computer monitor from discoloring. Screensavers have multiple uses today, one of which is security. If an employee leaves his/her workstation for a period of time, the computer can be programmed to launch the screensaver program. Screensavers can also be password-protected to prevent unauthorized individuals from accessing sensitive information.

Secure Electronic Environment
An environment that has administrative procedures, physical safeguards, and technical security services and mechanisms in place to prevent unauthorized access to EPHI.

Security or Security Measures
Encompasses all of the administrative, physical, and technical safeguards in an information system (e.g., passwords, firewalls, backups, etc.).

Security Incident
The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Smart Card
A type of plastic card similar to a credit card, but embedded with a computer chip that stores data. Users can be authenticated and authorized to have access to specific information based on preset privileges stored on the chip. Only computers that have a reader as part of its system read the data stored on the card.

System
Normally includes hardware, software, data, applications, and means of communication.

Technical Safeguards
Processes that are implemented to control and monitor access to EPHI such as passwords, as well as limit unauthorized access to data that is transmitted over a communications network (Internet, Intranet, fax, etc.).

Third Party Administrator (TPA)
An entity that processes healthcare claims and performs related business functions for a health plan.

Time-of-Day Access Control

Access to data is restricted to certain periods, e.g., Monday through Friday, 8:00 a.m. to 6:00 p.m. This is a function of audit controls that allows the practice to determine exactly when the system was accessed.

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.

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.

User
A person or entity with authorized access.

User ID
A unique identifier given to an individual allowing that individual access to a computer system. A User ID is usually accompanied by a password.

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.

Workstation
A computer used for running software applications, storing, and transmitting data. In networking, workstation refers to any computer connected to a local area network.

Step-By-Step Guide to the Security Rule

In order to ensure compliance with the Security 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. See also Exhibit 2.

Date Completed	
_____	Read the Overview of the Security Rule
_____	Appoint a Security Official/Prepare & Implement Job Responsibilities
_____	Perform Risk Analysis
_____	Determine if Computer System is Capable of Providing Electronic Audit Trails/Implement Audit Control Policies & Procedures
_____	Develop Workforce Clearance Procedures and Means of Implementing Clearance Requirements for Employees Who Access EPHI
_____	Design and Implement User Identification and Authentication Policies and Procedures for Electronic Information Systems
_____	Implement Automatic Log-off Processes
_____	Implement Transmission Security/Encryption Technology
_____	Install Protection from Malicious Software; Report Security Incidents
_____	Implement Firewall Technology
_____	Review and Implement Computer Backup Policies and Procedures
_____	Develop Security Incident/Breach Policies and Procedures
_____	Implement Facility Maintenance Log
_____	Develop Facility Security and Contingency Plans

Date Completed	
_____	Develop a List of Business Associates and Implement Business Associate Agreements
_____	Create Computer Workstation Use Policies and Procedures
_____	Document and Train All Physicians and Staff on the Security Policies and Procedures
_____	Obtain Signed Workforce Confidentiality Agreements from Physicians and Staff
_____	Monitor Compliance with the Security Rule
_____	Evaluate All Policies and Procedures Periodically
_____	Create Workforce Termination Procedures
_____	Implement Sanction Policy

Step 1: Read the Overview of the Security Rule

On August 12, 1998, the Department of Health and Human Services (HHS) published the proposed Security and Electronic Signature Standards. The statutory requirements are contained in the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). On February 20, 2003, HHS promulgated the HIPAA final Security Standards (Security Rule). On April 21, 2003, the Security Rule became effective with a compliance date of April 21, 2005. (Originally, the proposed Security Rule had two major components: the Security Standard and the Electronic Signature Standard. However, the Electronic Signature Standard was removed from the Final Security Rule.) The Security Rule was further modified by the Health Information Technology for Economic and Clinical Health Act (HITECH), passed as part of the American Recovery and Reinvestment Act of 2009 (ARRA).

Healthcare plans, providers, and clearinghouses, along with the business associates of such covered entities that participate in programs administered by HHS, other Federal agencies, and state Medicaid agencies must comply with the Security Rule. As such, healthcare plans, providers, and clearinghouses are required to assure the confidentiality, integrity and availability of individuals' electronic protected health information (EPHI).

Background: General Privacy Concepts: the Privacy Rule vs. the Security Rule.

WHAT IS A COVERED ENTITY?

A covered entity means a health plan or payor (including government payers), 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) that conduct transactions covered by HIPAA electronically (e.g., electronic claims billing or verification of eligibility electronically).

The main purpose of the Security Rule as stated by the Department of Health and Human Services is to create national standards to protect the confidentiality, integrity, and availability of electronic protected health information.

PRIMARY PURPOSE OF THE SECURITY RULE:
To protect the confidentiality, integrity, and availability of electronic protected health information.

Prior to the Security Rule, patients had no nationally standardized legal protection for the electronic security of their medical records. With continued advances in electronic technology, including expanded use of the Internet as a business tool, there is growing concern among the general public regarding the confidentiality of their health information. The Security Rule requires security protection for patients' electronic protected health information.

Electronic Protected Health Information

WHAT IS EPHI?

Electronic Protected Health Information (EPHI), is PHI that is:

1. transmitted by electronic media, or
2. maintained in electronic media.

Protected Health Information

WHAT IS PHI?

Protected Health Information (PHI) is a subset of **Individually Identifiable Health Information (IIHI**). IIHI is 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 could potentially identify an individual.

PHI is IIHI , excluding education records under the Family Education Rights and Privacy Act (FRPA); records described at 20 U.S.C. § 1232G(a)(4)(B)(iv) (psychotherapy records under FRPA); and employment records held by a covered entity as an employer.

The Security Rule encompasses all data that is created in an electronic format with regard to protected health information (PHI) as addressed by the Privacy Rule. So, it is important to consider how the two standards work hand in hand.

EXAMPLE OF THE PRIVACY AND SECURITY RULE WORKING TOGETHER

Creating a document to be faxed:

1. A document is created in the practice‘s computer system.
2. The Security Rule addresses and protects that document as long as it is maintained within the computer system.
3. If the practice‘s computer system has fax capabilities, the Security Rule addresses and protects that document as It is transmitted.
4. For the document that is printed in order to be transmitted via fax machine, the Privacy Rule then addresses and protects the document.

Note

Telephone voice response and ”faxback” systems (requests from a computer made via voice or telephone keypad input with the request information returned as a fax) **are** covered under the Security Rule.

Paper to paper faxes, person-to-person telephone calls, video conferencing, or messages left on voicemail are not covered by the Security Rule.

WHAT DOES "ACCESS" MEAN?

Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource that creates, maintains, or transmits EPHI.

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 collections, marketing and technology services. Many of these types of entities may be identified under the Security Rule as "Business Associates."

WHAT IS A BUSINESS ASSOCIATE?

A person or entity that is not a member of your practice's workforce who creates, receives, maintains, or transmits electronic protected health information to carry out certain functions or activities on behalf of the practice.

See Exhibit 14 for a list of typical Business Associates and Exhibit 15 for a flow chart to help identify Business Associates specific to your practice. 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. Business Associates are required to comply with many of the Security Rule's provisions.

The Security Rule

The Security Rule establishes requirements regarding the medical practice's creation, receipt, storage, maintenance, and transmission of EPHI in a secure electronic environment. It applies not only to the transactions adopted under HIPAA, but also to ALL EPHI that is maintained or transmitted by a covered entity. As noted above, the Security Rule does not apply to PHI that is transmitted in certain forms, including paper via facsimile, or via voice by telephone.

WHAT IS A SECURE ELECTRONIC ENVIRONMENT?

A **Secure Electronic Environment** is an environment that has administrative procedures, physical safeguards, and technical security services and mechanisms in place.

Security Rule Implementation

Medical practices are not required to implement the Security Rule in any particular order and can therefore do so in a manner that best suits the individual practice. However, because many of the components of the rule are co-dependent, we strongly suggest that you implement the Rule's requirements in the order that they are presented in this manual.

Importantly, the Security Rule is "technology neutral." This means that it neither refers to nor advocates the use of specific technology such as certain information systems, hardware, or software in order to achieve compliance with the Rule. **A medical practice is encouraged to speak with each computer vendor that it uses to verify that vendor's ability to provide a software or hardware solution that adequately addresses the practice's compliance obligations under the Security Rule. The Practice should also remember that the Security Rule impacts more than just the practice's technology solutions. Traditional physical attributes of the practice are also covered by the Rule (e.g., the practice's building, office locks, premises safety, etc.)**.

THE PRACTICE'S GENERAL OBLIGATIONS UNDER THE SECURITY RULE

Under the Security Rule, a Covered Entity must:

- Ensure the confidentiality of all EPHI that it creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.
- Ensure compliance with the Security Rule by members of its workforce.

Means of Complying with the Security Rule

The Security Rule was purposely written broadly. The specific security measures that one practice uses to comply with the Rule may vary from the specific measures taken by another practice. For example, the security measures used by a 30 physician, multi-specialty practice with seven locations will likely be quite different from those used by a two physician, single- specialty practice with one location. However, the process set forth in this manual is applicable to all medical practices.

In deciding what specific security measures to use in order to comply with the Security Rule, each practice must consider the following:

1. The size, complexity, and capabilities of the practice.
2. The practice's technical infrastructure, hardware, and software security capabilities.
3. The cost of security measures.
4. The probability and criticality of potential risks to EPHI.

As the Practice evolves, it must document and keep current the security measures. In addition, practices are required to maintain their documentation for six years.

Specific Components of the Security Rule

THE SECURITY RULE IS DIVIDED INTO THREE PRIMARY SAFEGUARDS

Administrative Safeguards are formal, documented practices to protect EPHI. This includes the selection and execution of security measures and the management of personnel as it relates to protecting EPHI.

Physical Safeguards are procedures to protect computer systems, buildings, and other equipment from fire and other natural and environmental hazards, as well as from intrusion.

Technical Safeguards are processes that are implemented to control and monitor access to EPHI, such as passwords, as well as limit unauthorized access to data that is transmitted over a communications network (Internet, Intranet, fax, etc.).

Within each of these primary safeguards are standards that practices are required to meet. Many of these standards are broken down further to give practices some flexibility in satisfying the Security Rule. These are called Implementation Specifications. There are 39 specific implementation specifications necessary for full compliance with the Security Rule.

Addressable and Reasonable

Importantly, the implementation specifications set forth in the Rule are either **required** (there are 20 of these) or **addressable** (there are 22 of these) by the practice. Although practices are required to document their decisions for each Implementation Specification, the **addressable** specifications grant practices some flexibility.

The flexibility of the Security Rule means that the specific security measures used by various practices will vary. See Exhibit 2 for a cross-reference matrix of the Security Rule components, standards, and the contents of this manual. In addition, each step within the manual contains a Snapshot Compliance Matrix, specifically identifying the components of the Rule addressed by the particular step. Within that matrix, **addressable** specifications are noted by an "A", and **required** specifications are noted with an "R".

To clarify further, practices should reference Appendix 1. It is important to remember that all Standards must be met either by conforming with a specific implementation specification or by some other means. Most Standards have Implementation Specifications.

Implementation specifications that are noted as **required must** be implemented by the practice.

Implementation specifications that are noted as **addressable must** be satisfied by the following process:

First, decide if the addressable specification is reasonable and appropriate to implement in your practice. Is it likely to contribute protection to the practice's EPHI?

Second, if the specification is reasonable and appropriate, as it is written, then you must implement the specification. If the specification is not reasonable and appropriate for your practice as it is written, you must:

- Document why the specification is not reasonable and appropriate as it is written and implement a reasonable and appropriate equivalent alternative or

- Document why the specification does not apply to your practice and how the security standard is otherwise being met.

It is important to remember that all decisions must be documented. In addition, you should keep in mind that as your practice evolves (not just financially, but also with the acquisition of new technology), it will be necessary to reevaluate periodically compliance with the Security Rule. Over time, it is likely that the specific security measures used by the practice in order to comply with the Rule will change.

Note

What is reasonable and appropriate for a small practice may not apply to a larger practice. For example in a solo practice, the use of passwords is reasonable and appropriate while using biometric identifiers, such as fingerprints, is not.

The Relationship Between HIPAA and State Security Laws

Many state security laws will continue to apply and be enforced following the public declaration of the HIPAA security rule. 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.

Many states currently have laws regarding the security of health information. It is a huge task to determine how the state‘s security requirements compare to the federal HIPAA requirements. 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 security.

You should think of HIPAA as a federal security ”floor,” since the regulations represent a national set of minimum standards. Generally speaking, a federal security ”floor” means that if a state‘s laws are not as stringent as HIPAA, then the federal security regulations will apply. In the event that a state‘s laws are more stringent or provide greater security 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).

Step 2: Appoint A Security Official, Prepare and Implement Job Responsibilities

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	**Required vs. Addressable**
Administrative	Assigned Security Responsibility	None	Required

See Exhibit 1: Security Official Job Responsibilities.

See Exhibit 1A: Privacy and Security Official Job Responsibilities.

The Security Rule **requires** the Practice to designate a Security Official who is responsible for the development of the policies and procedures required by the Rule.

The Security Official will have final responsibility for the practice's security compliance. 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 Security Rule. If your practice is organized as a separate legal entity (such as a corporation or partnership),
you should also specifically indicate the name of the person that you have appointed to be the Security Official for the year within the entity's corporate minutes.

In conjunction with the appointment of a Security Official, the practice should clearly define the Security Official's duties and responsibilities in a similar form used for the practice's other job descriptions. By outlining the specific duties and obligations, the parties will each fully understand what is expected of them in the practice's efforts to maintain compliance with the Security Rule.

In smaller practices, the office manager or other designated individual will typically assume the duties of the Security Official within his/her current job as they have likely assumed the role of Privacy Official. For larger practices, it may be necessary to designate an additional full- time employee as the Security Official. It is the responsibility of the individual practice to determine whether or not it should designate an additional full-time employee for this position.

To Do

- Identify your Security Official:

Practice Name:_____

Name of Security Official:_____

Date:_____

- Document the name of the Security Official in the practice's corporate minutes.
- Fill in your Practice Name on either Exhibit 1 or Exhibit 1A.
- Document when Security Official responsibilities are adopted and/or revised.
- Security Official responsibilities were:

Adopted:_____
Date

Revised:_____
Date

Revised:_____
Date

The Security Official may also be the same person who has been designated as the Privacy Official, in compliance with the Privacy Rule.

• The Security Rule does not require that an additional employee be hired to perform these duties. The Security Rule mandates that one person be accountable for the practice's compliance with the Rule. However, the Security Official can delegate responsibilities to other employees or an outside vendor, if necessary. It is up to the practice to determine whether or not they need to hire someone specifically to be the Security Official or to have a current employee absorb the duties into his/her job description.

• Practices may consider sharing a Security Official or outsourcing these responsibilities to an outside entity, such as an information technology (IT) consultant or vendor.

• As bigger practices move further into the use of electronic information technologies, it may be appropriate to develop an in-house IT position. The responsibilities of this position may include staff training, system monitoring, and naturally, HIPAA Security.

• As the practice evolves, the practice's on-going security analysis may indicate that the Security Official's responsibilities may need to be modified as a partial response to the practice's modified means of compliance with the Security Rule.

• As additional clarification of the Security Rule is provided by HHS, these responsibilities may need to be modified.

• Place this form and other relevant forms in a permanent HIPAA Security folder or binder to serve as part of your practice‘s overall Compliance Plan.

Step 3: Perform a Risk Analysis

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	**Required vs. Addressable**
Administrative	Security Management Process	Risk Analysis	Required

See Exhibit 2: HIPAA Security Rule Standards Matrix & Risk Analysis

The practice is required to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI that it holds. A thorough assessment consistent with the Rule will encompass more than just the practice's computer systems. The risk analysis must consider all relevant losses that would be expected if the risk measures were not in place. "Relevant losses" would include losses caused by unauthorized uses and loss of data integrity that would be expected to occur absent security measures implemented by the practice.

The Security Official should use the Risk Analysis provided in Exhibit 2 as a guide to auditing the practice and preparing it for compliance with the Rule. This is an important early step since the practice's answers/results of the analysis will impact other steps throughout the manual.

To Do

- Fill in your Practice Name on Exhibit 2.

- Photocopy Exhibit 2 (all pages) for each practice location. (Keep a master copy for future quarterly or annual assessment reviews.)

- Follow the checklist.

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

Note

- If multiple locations are operated by your practice, this audit must be conducted at each location.

- It may be necessary to seek input from IT support vendors to determine compliance with certain security requirements.

- The Risk Analysis checklist allows your practice to document your decisions for both required and addressable specifications.

- Place this audit tool in a permanent HIPAA Security Rule folder or binder to serve as part of your practice's overall Compliance Plan.

The Risk Analysis allows you to clearly identify and document your decisions regarding the 22 addressable specifications. Once complete, file the checklist in your HIPAA Security Folder and maintain the completed Risk Analysis (and subsequent revision to the Analysis) for six years. The Risk Analysis should be reviewed periodically based on the changes and evolution of the practice.

Step 4: Determine if Computer System is Capable of Providing Electronic/Audit Trails; Implement Audit Control Policies and Procedures

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation on Specification**	**Required vs. Addressable**
Technical	Audit Controls Transmission Security	None Integrity Controls	Required Addressable
Administrative	Security Management Process	Information System Activity Review	Required

See Exhibit 3: Sample Audit Trails Policy & Procedures.

See Exhibit 4: Sample Event Record.

In addition to Step 3, "Perform a Risk Analysis", Step 4 is one of the more crucial steps for practices to implement. The Security Rule **requires** the practice to implement hardware, software, and/or procedural mechanisms that record and examine activity and information systems that contain or use EPHI. The Practice should refer to Exhibit 2 (Risk Analysis) to determine exactly how intensive the audit control function should be.

Some practices will find that their current practice management and electronic medical records software can produce an electronic audit trail. Under these circumstances, Step 4 is quite easy to implement. However, for those practices that are not so lucky, Step 4 may take some time.

Practices should look at their programs that contain EPHI and determine whether or not it can produce an electronic audit trail. Electronic audit trails are computer programs that allow the computer to track, identify, and record which individuals have accessed the computer system and what activities they have performed while using the computer system. In conjunction with other security tools and procedures, electronic/audit trails can provide the practice with comprehensive information about technical, procedural, and managerial aspects of the practice's security program. An electronic audit trail will be one way to assess activities regarding EPHI contained in the practice's computer system.

The audit trail also serves as a mechanism for employee and workforce accountability as it tracks who and when employees have accessed computer software programs, what programs they have accessed, and what activities they have performed while logged into the computer system. The audit trail should include information to establish and record who accessed the practice's computer system, when the computer system was accessed, what software programs were accessed, and any other activities that occurred within the system. This is typically done through an "event record." The event record should, at a minimum, include the following items:

- Type of event. For example, an unauthorized access to a particular portion of the practice management system for which the employee has not been granted permission to access;
- When the event occurred, including time and day (the practice should determine whether its computer system is capable of date and time stamping such events);
- Which User ID is associated with the event;
- What part of the computer system was used to start the event? For example, did an event occur because an employee accessed the billing component of the practice's system instead of the clinical component of the system?

Note

•Determine if your computer system can generate an audit trail. Contact practice management and/electronic medical records vendor(s), if applicable, and ask.

•If the computer software program(s) can generate an audit trail, determine how to activate this function.

1. Activate the computer software program's audit trail function.
2. Review audit reports weekly.

•If the computer software program(s) cannot generate an audit trail, contact the computer software vendor(s). It is a requirement of the Security Rule that covered entities have this capability.

•Designate an individual in the practice to maintain the audit trail process. Ideally, the individual responsible for assigning and maintaining User IDs and access control processes should be different from the individual maintaining the audit trail functions, but in smaller practices, this is not always possible.

•Create an event record to establish what event occurred, when it occurred, with whom it is associated, and what part of the system was potentially compromised. (See Exhibit 4).

•Develop policies and procedures to address conducting and implementing audit trails. (See Exhibit 3).

Note

•Electronic audit capabilities are required by the Security Rule

•The computer software programs that store EPHI must be able to produce the electronic audit report. It is not required for your computer system in general.

•Comprehensive audit trail policies and procedures should include several important components, including the ability to:

1. Identify and track which employees accessed the practice's computer system, when they have accessed it, what they accessed, and what (if any) actions were taken by those individuals (e.g., changes to EPHI);
2. Assist in detecting unauthorized access to the practice's computer system or unauthorized access to software programs that an employee does not have access to;

3. Identify problems with the computer system, other than intrusions, and reconstruct unfortunate events that may have occurred as a result of unauthorized access to the computer system.

- Depending on the computer software used to perform it, an audit trail can be tracked and monitored in ”real time”, i.e., the same time that the employee logs into the computer and accesses the computer system and its software programs.

Step 5: Develop Workforce Clearance Procedures and Means of Implementing Clearance Requirements for Employees who Access EPHI

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	**Required vs. Addressable**
Administrative	Information Access Management	Access Authorization	Addressable
Administrative	Information Access Management	Access Establishment and Modification	Addressable
Administrative	Security Awareness and Training	Password Management	Addressable
Administrative	Workforce Security	Authorization and/or Supervision	Addressable
Administrative	Workforce Security	Workforce Clearance Procedure	Addressable
Technical	Access Control	Unique User Identification	Required
Technical	Person or Entity Authentication	None	Required

The practice must implement policies and procedures to ensure that all members of its workforce have **appropriate** access to PHI (including EPHI) and prevent those who do not need access from obtaining access. This is **required** under the Privacy Rule as well as the Security Rule.

In order to satisfy the Workforce Security Standard requirement, practices must look at two implementation specifications: Authorization and/or supervision and workforce clearance procedure. Both of these implementation specifications are **addressable**.

Practices may find it helpful to refer back to page 23 in order to review how to implement an **addressable** implementation specification.

Note

Authorization and/or Supervision:
The practice must address what procedures to implement for the authorization and/or supervision of the workforce members who work with EPHI or who work in locations where it might be accessed.

Note

Workforce Clearance Procedure:
The practice must also address what procedures to implement to determine whether a member of the workforce's access to EPHI is appropriate. It may be necessary for all staff of smaller practices to have access to all EPHI in order to carry out their job responsibilities. On the other hand, in a larger practice, it may be more feasible to limit access to certain EPHI to certain individuals.

The development and issuance of job descriptions for each of the workforce members and the use of background checks on current and prospective workforce members are two acceptable means of accomplishing both of these **addressable** specifications.

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 each needs to PHI (including EPHI). Job descriptions should be routinely reviewed for accuracy and appropriateness.
Consistent with the Privacy Rule, job descriptions should address the **minimum necessary** access required by a person or job title in the practice that must have access to EPHI to carry out their duties. Once this is identified, the category or categories of EPHI to which these persons need access must be identified. For example, certain employees will need access to patients 'financial information contained in the billing system while other employees may not. The purpose of this exercise is to identify the minimum necessary level of access to EPHI needed by individuals in the practice to carry out their job responsibilities.

The practice policies and procedures governing access levels to EPHI 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 EPHI **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 that 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.

Authorization procedures may include, among other efforts, background checks, credit checks, and/or other means of personnel screening in order to determine whether it is appropriate for certain members of your workforce to access EPHI. The practice should consider the risk, cost, benefit, and feasibility of certain means of workforce clearance procedures, both before (as prospective employees) and during an individual's employment or other engagement with the practice.

To Do

<u>Job Descriptions</u>
• Review current position descriptions and add minimum necessary standard EPHI requirements. Specifically, state what the employee is expected to access in order to perform his/her duties.

• If job descriptions do not exist in your practice, you should develop them or, at the very least, a job description should consist of separate written statements or documents outlining the minimum necessary access to EPHI requirements for each position, and what is expected to be accessed by the individual.

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

Background Checks

• Identify the practice's current means of conducting background and employment referral checks.

• Standardize the consistent use of an identified means of conducting background checks on prospective employees.

• Consider whether it is appropriate to conduct background screening on some or all current employees.

Training

• Employee Security Rule training should include a review of his/her new job description (inclusive of EPHI security levels). Employee should sign a statement acknowledging that they have read and understand the job description.

To Do

Security Officials Responsibility

• The Security Official should maintain a master employee list as well as the authorized levels of access to patient information and computer passwords for each employee.

• Develop a policy outlining disciplinary actions to be taken by the practice against an employee who accesses EPHI beyond his/her need to know (security) level as outlined in his/her job description.

Note

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

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

• Some appropriate websites that practices can access in order to implement personnel screening are the OIG and GSA sites, http://exclusions.oig.hhs.gov and https://explore.data.gov/d/bxfh-jivs respectively. Both of these sites are free and take only a matter of minutes to check.

• There are companies that will conduct credit and criminal background checks for a fee.

Step 6: Design and Implement User Identification and Authentication Policies and Procedures for Electronic Information Systems

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	**Required vs. Addressable**
Administrative	Information Access Management	Access Authorization	Addressable
Administrative	Information Access Management	Access Establishment and Modification	Addressable
Administrative	Security Awareness and Training	Password Management	Addressable
Technical	Access Control	Unique User Identification	Required
Technical	Person or Entity Authentication	None	Required
Technical	Integrity	Mechanism to Authenticate FPHI	Addressable
Physical	Facility Access Controls	Access Control and Validation Procedures	Addressable

See Exhibit 5: Sample Policy for User Identification (User ID) and Authentication.

In order to protect EPHI, the practice must have a consistent and practical means of limiting access to EPHI. Access may be limited by a variety of security measures, though the most prevalent is the use of specific means to accurately identify and authenticate the identification of all EPHI uses, such as a User ID and password.

The rule includes a standard to implement policies and procedures for authorizing access to EPHI that are consistent with the Security Rule. However, the standard allows practices some flexibility. If necessary, refer back to page 23 to review how to implement an **addressable** specification.

Identification and authentication are technical measures that prevent unauthorized people (or unauthorized processes) from entering an electronic information system. Simply put, identification is a User ID and authentication is most commonly a password. User identification and authorization allow a computer system:

- To identify and differentiate among users;
- To ensure that only authorized individuals gain access to specific information systems resources;
- To assign individuals an appropriate level of privilege; and
- To hold individuals accountable for their actions.

Access to the practice's computer system should be controlled and limited based on positive identification and authentication mechanisms.

WHAT IS IDENTIFICATION?
Identification is the process that enables a computer system to recognize a computer user. The most common form of identification is a User ID.

WHAT IS AUTHENTICATION?
Authentication means the corroboration that a person is the one he/she claims to be. Authentication processes or mechanisms are those that are utilized to verify the identity of a person. The most common form of authentication is a user's password.

Identification consists of assigning a unique User ID and Password to each computer user. This allows the practice to control and track who has access to the practice's computer system. The practice should control access to the computer system itself and may also grant employees access to only the information that is minimally necessary for him/her to perform his/her job responsibility. A unique User ID and Password links activities on a computer system to specific individuals and therefore allows the system to identify individual computer users.

THREE WAYS TO VALIDATE A USER'S IDENTITY (AUTHENTICATION)
Something the employee knows
- password (most common)
- personal identification number (PIN)
- cryptographic key

Something the employee possesses
- token
- smart card

Biometric identifier
- fingerprints
- voice patterns
- handwriting dynamics

Passwords are the most common authentication tools used and are frequently used in medical practices. A computer password is a personal key to a computer system. They help determine accountability for all transactions and other changes made to the computer system including data. Most practices will utilize this method, however, as technology continues to evolve, practices may see biometric identifiers becoming more common.

If a practice employee shares his/her User ID and/or password with a colleague or friend, he/she may be giving an unauthorized individual access to the practice's computer system. It is recommended that practices consider using a combination of the previously mentioned methods for verifying an individual's identity to make it as difficult as possible for an unauthorized individual to access the practice's computer system.

To Do

The Security Official and/or System Administrator must:

• Implement policies and procedures User IDs and passwords. (See Exhibit 5)

• Establish User IDs for each practice employee.

• Document the User ID for each employee and file with computer system records.

• Establish an initial password for each employee. Upon receipt of the initial password, employees will be provided the opportunity to change their password. If employees are given the opportunity to change the provided password; they must also give this new password to the Security Official.

• Distribute the initial password to each employee in a confidential manner (e.g., by using a sealed envelope or leaving a voicemail message in a confidential voice mailbox).

Training

• Instruct employees either to use the password assigned to them or create a new password in accordance with the practice's procedures for creating secure passwords.

• Distribute Exhibit 5 to employees.

• Review "Note" box with employees.

Note

The following guidelines should be utilized when instructing employers to create their own passwords.

• Use a password that is easy to remember so it doesn't have to be written down.

• Use of alpha-numeric passwords or special characters like #, $, and @ are more secure than using just letters or just numbers.

• Do not use his/her login name in any form (e.g., as-is, reversed, capitalized, doubled, etc.). Do not use the employee's personal name, a family member's name, or any other personal identifier, such as a birth date, street address, etc.

• Use a password that he/she can type quickly, without having to look at the keyboard. This makes it harder for someone to steal a password by watching over your shoulder.

Step 7: Implement Automatic Log-Off Processes

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	**Required vs. Addressable**
Technical	Access Control	Automatic Log-off	Addressable

In addition to utilizing User IDs and passwords to ensure that initial access to the computer system is secure, practices must consider additional mechanisms to prevent unauthorized access to the computer system at times other than initial access. The Security rule requires practices to implement access controls, but allows some flexibility. In order to satisfy the access control standard, practices must determine if the use of Automatic log-off procedures are both appropriate and reasonable for the practice.

If an employee must leave his/her workstation for an extended period of time, he/she should log off the computer system. If the employee does not log out of his/her computer prior to leaving the workstation and is away from his/her workstation for longer than anticipated, there is the potential for another individual to access and utilize the computer software.

To prevent access to the computer by anyone but the assigned employee, the practice should consider activating or implementing technology that has an automatic time-out feature, such as automatic logoffs or password-protected screensavers. Automatic logoffs or password- protected screensavers make the employee‘s computer inaccessible to an unauthorized individual after a period of keyboard inactivity. The length of the period of inactivity triggering the time-out feature should be determined by the sensitivity of the application.

WHAT IS AN AUTOMATIC LOG OFF?
An automatic log off is the process that a computer server uses to disconnect a connection to the computer server when no data has been transmitted for a given period of time.

WHAT IS A SCREENSAVER?
If an employee leaves his/her workstation for a period of time, the computer can be programmed to launch the screensaver program. Screensavers can also be password-protected to prevent unauthorized individuals from accessing sensitive information.

Security Official

- Determine if the practice will utilize automatic log-off and/or screensaver technology to prevent unauthorized access to an employee workstation while it is unattended.

- If the practice decides to utilize automatic log-off and/or screensaver technology, the practice should install “locking software” that can be set to activate after a period of time of computer keyboard inactivity. The software will log an employee out of the system after this period of time. The employee will have to enter his/her User ID and password in order to regain access to the computer system.

- If the practice decides not to utilize automatic log-off and/or screensaver technology, the practice needs to document its decision not to implement on (see Exhibit 2).

- When an employee leaves the practice, disable his/her User ID and password immediately in accordance with the user identification and authentication policies and procedures and workforce termination procedures. (See Exhibits 5 and 21.)

Training

- If implementing automatic log-off function, instruct employees on its use.

It is **reasonable** and appropriate for practices of all sizes to implement at a minimum, password protected screensavers as a means of automatic log-off.

Important note:

• Automatic log-off and password protected screensaver features can sometimes be evaded by restarting the computer. It is critical, therefore, that the practice have in place and utilize strong user identification and password policies and procedures.

• Once an employee returns to their workstation that has an automatic log-off function and logs back into their computer, they will no longer be in the application that they were previously. Password protected screensavers allow the employee to pick up where they left off prior to leaving their workstation.

Step 8: Implement Transmission Security / Encryption Technology

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	**Required vs.**
Technical	Access Control	Encryption and Decryption	Addressable
Technical	Transmission Security	Encryption	Addressable

The Security Rule includes a standard to implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that are granted access, consistent with the parameters of the Security Rule.

The Security Rule also includes a standard to implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network (e.g., the Internet). Both the Access Control and Transmission Security Standards include implementation specifications regarding encryption and decryption that are **addressable.** To be compliant with both Standards, practices must decide if the use of encryption and decryption software is **reasonable** and appropriate.

EPHI has been encrypted as specified in the Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST), and HHS judges such processes to meet Security Rule standards.

(i) Valid encryption processes for data at rest that are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.

(ii) Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are validated per Federal Information Processing Standards (FIPS) 140-2.

If your practice utilizes email to send EPHI over the Internet to others, including providers, patients or vendors, the practice is not required to use encryption, but it must at least consider encryption or other protective alternatives. (It is an "addressable" implementation specification.) Encryption software will protect the information contained in the email message or the computer files that may be attached to the email and ensure that neither may be accessed and/or changed while the message is in transit over the Internet.

Encryption is also the method used to render EPHI "secured." As noted, encryption is not absolutely mandated by the Security Rule. However, it could save your practice a significant amount of time, effort and expense should any type of unpermitted disclosure or other "Breach" occur. This is because the Breach Notification Rules apply to only breaches of "unsecured" PHI. "Unsecured PHI" is 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.

In other words, a non-permitted use or disclosure of encrypted PHI is not a "breach" under the Security Rule. Therefore you are not required to notify patients or others of such disclosure, under the Breach Notification Rules.

The practice has several alternatives with respect to email: (1) do not use it at all, (2) clearly define and limit the purposes for which email can be used, e.g., not for discussion of patient clinical issues (3) allow broader use of email, such as exchange of clinical information with patients, but have the patient consent to using unsecured email and include how email is used in the NPP, (4) use a secure service, or (5) obtain encryption software.

Note

WHAT IS ENCRYPTION AND DECRYPTION?
Encryption is a process used by a computer to encode a readable message in order to prevent anyone except the intended recipient from reading it. In order to read the message, the recipient must be able to **decrypt** or decode the message using a special set of numbers or characters called a key. A message typically starts out in plain text, is encrypted into what is referred to as "ciphertext" and sent to the recipient. The recipient uses a key to decrypt the message back into plain text so it can be read and understood. There are different types of encryption and decryption software that can be implemented based on the type and amount of information to be sent.

Different encryption software programs have different ways of encoding and decoding data. These programs offer different features depending on the sensitivity level of information that is being transmitted.

Additionally, some encryption software programs require the recipient of an encrypted document or email message to use the same software the sender used. Others simply require the recipient to possess the same key or password that the sender used.

Note

• Determine if your practice utilizes email or plans to utilize email to transmit EPHI over the Internet.

• If the practice uses or intends to utilize email to communicate with other covered entities, patients, vendors or other parties, the practice must consider installing encryption software or implementing alternative measures of protection. The practice should consult an information technology specialist to determine the appropriate software product given the information the practice intends to transmit via email.

• Because utilization of encryption software is an addressable implementation specification, if the practice does not intend to implement encryption software, the practice needs to document this decision (see Exhibit 2).

Note

• It is reasonable and appropriate to install encryption software if the practice is emailing EPHI. It is also reasonable to implement another alternative as previously mentioned.

Step 9: Install Protection from Malicious Software; Report Security Incidents

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	**Required vs. Addressable**
Administrative	Security Awareness and Training	Protection From Malicious Software	Addressable
Technical	Transmission Security	Encryption	Addressable
Administrative	Security Incident Procedure	Response and Reporting	Required

See Exhibit 7: Security Incident Report.

The Security Rule includes a standard to implement policies and procedures regarding security incidents. In particular, the practice is required to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the practice; and document security incidents and their outcomes. The easiest way to protect your EPHI from security incidents is to install virus scan software.

Computer viruses are malicious software programs or sets of instructions that have been written to purposely cause harm to computer systems, networks, and the information that resides on them by copying themselves from one computer to another.

Viruses are often written to masquerade as useful software programs and can inadvertently be passed on as computer files that are copied and shared. Viruses are often hidden within files that you may receive from the Internet, a colleague, a friend, or some other outside source such as your own home computer. The damage caused by viruses can vary widely and can be so extensive as to require the complete rebuilding or replacement of a computer system and the data it contained.

As soon as a virus is loaded into your computer, it can be quickly spread to other programs on your computer and with computers that you may share information. For example, if your computer at home is infected with a virus and you save information from your computer to a storage device such as a thumb drive and insert the drive into the practice‘s computer, you may have transferred the virus to the practice‘s computer.

Because of the potential damage a virus can cause to the practice‘s computer system, the practice is strongly encouraged to consider implementation of anti-virus software or software that can scan the computer and its files and identify harmful software programs. Anti-virus software constantly monitors, locates, and identifies known computer viruses. It checks certain types of files on your computer whenever you access those files. It can also be used to scan external drives and storage devices manually, which should be done whenever you connect a portable storage device from someone else or bring one from home. If the anti-virus software detects a virus on a computer or storage device, it informs you that your computer system has a virus. As a result of the myriad of features available with most anti-virus software, use of such software will meet both the **addressable** and **required** elements addressed by this step.

The Security Rule includes a standard to implement a security awareness and training program for all members of its workforce. A component of this awareness and training may include virus scan software and guidance regarding its use by members of the workforce. The practice must **address** whether or not it is appropriate and **reasonable** for the practice to implement procedures to detect and report malicious software events.

- Fill in your practice name on Exhibits 6 and 7.
- Determine if you intend to use anti-virus software. If not, document your rationale for this decision (see Exhibit 2).
- If you intend to use anti-virus software, select anti-virus software.
- Install and run anti-virus software on the following technology components:

  – Desktop or personal computers (PC)
  – Computer servers
  – Laptop and portable computers

- Configure anti-virus software to check for viruses in computer files, computer disk drives (e.g., hard drive), email messages, portable storage devices, and information downloaded from the Internet.
- Configure anti-virus software to send a message automatically to the computer user that a virus has been deleted and to log and remove the virus automatically from the infected computer files, disk drives (e.g., hard drive), email messages, and any information stored on the computer that has been downloaded from the Internet.
- Complete security incident report (Exhibit 7) when a virus is discovered in the practice‘s computer system and take appropriate steps to stop the virus from infecting other parts of the practice‘s information system.
- Implement procedures to recognize computer viruses and reduce the risk of computer viruses disrupting practice operations. (See Exhibit 6.)
- The implementation of policies and procedures to identify and address security elements is required. Use of appropriate anti- virus software will appropriately satisfy, in part, this requirement.

Note

• When staff detects a virus, they must cease work on their workstations and contact the system administrator or Security Official immediately. Employees should not try to correct suspected virus-related issues unless they have been given specific prior authorization.

• No anti-virus software program provides one hundred percent protection from computer viruses. It is imperative that all necessary precautions are taken to avoid infecting the practice‘s information system. The practice should take precautions to minimize infection including scanning all incoming and outgoing storage devices and not downloading information from unfamiliar or unknown sources or Internet web sites.

• Some viruses hide themselves within the computer system and do not give the computer user any indication of their presence while others are more recognizable.

• Other viruses come as attached files and are designed to spread themselves by opening Microsoft Outlook address books and mailing themselves to all the addresses in the address book.

Step 10: Implement Firewall Technology

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	**Required vs. Addressable**
Administrative	Security Awareness and Training	Protection From Malicious Software	Addressable

Consistent with the use of anti-virus and encryption software, the practice should consider installing firewall technology to protect its computer system.

A firewall is a computer software program or hardware device that filters information coming through an Internet connection into the practice's computer information system or network. A firewall works by flagging or identifying unwanted information and preventing unauthorized users and incoming information, such as email messages, from entering the practice's computer system.

In addition, the practice can use firewall technology to control how its workforce connects to Internet web sites and to determine whether computer files are allowed to leave the company over the network. A firewall gives the practice control over how people access and use the practice's information system. For example, you can ban staff from pornographic sites.

Different types of firewalls perform different functions and vary in terms of cost. The simplest types of firewalls are programmed to identify email messages from known, trusted sources. These fairly inexpensive firewalls will stop messages with inappropriate email addresses and block them from reaching the practice's computer system. More complicated firewalls can identify such messages, open any attachments, and screen the attachments for viruses. The practice will need to consider its information security requirements based on the Security Risk Assessment it conducted in Exhibit 2 to determine which firewall technology is best for the practice.

To Do

• Conduct Security Risk Analysis (see Exhibit 2).

• Determine whether the practice needs a firewall. If the practice does not have Internet access, it does not need a firewall.

• If the practice does have Internet access, the system administrator or security official will need to consider what type of firewall to implement. The system administrator or security official may need to enlist the assistance of an information technology consultant or vendor to determine the appropriate firewall technology.

• Make sure the firewall is the only connection between the practice's computer system and outside resources, such as the Internet, to ensure close monitoring of incoming and outgoing information. Be sure to eliminate any additional methods for employees to access the Internet from the practice, such as through the use of unauthorized modems.

• Perform the following necessary maintenance tasks after the firewall has been installed:

– Implement and review computer system audit trails (see Step 4) and activity logs generated by the practice's computer system to improve intrusion detection.
– Establish and document how frequently the computer system audit trails will be reviewed and be sure to conduct the reviews at the specified times.
– Note unusual patterns of Internet usage and investigate them.
– Follow up on alerts generated by the firewall.

• Test the firewall regularly to make sure that it is performing as expected. (It will have a testing function within the tools. Utilize the testing capabilities.)

• Use a firewall as part of the practice's overall network security solution. To fully protect the computer system, the firewall must be used in conjunction with the practice's policies and procedures and other technology solutions.

• While firewalls can block unauthorized users and file types from corrupting the practice's computer system, they cannot block viruses that have been transmitted through the Internet or by employees sharing infected computer files. A firewall also cannot protect against deliberate disclosure or intentional modification of data by authorized or unauthorized users.

• The practice may need to reconfigure the firewall as software applications are added, new protocols are implemented, employees leave or are hired into the practice, and/or as the computer system is upgraded.

Step 11: Review and Implement Computer Backup Policies and Procedures

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	**Require vs. Addressable**
		Data Backup Plan	Required
Administrative	Contingency Plan	Disaster Recovery Plan Emergency Mode Operations Plan	Required Required Required
Technical	Integrity	Mechanism to authenticate EPHI	Addressable

See Exhibit 8: Sample Backup Policy and Procedures.

As a component of the Risk Analysis, each Practice must determine its data backup needs. Many practices are already in the habit of backing up their data, but do not have a formal policy in place.

The Security Rule requires the Practice to establish policies and procedures for a data backup plan in order to protect the EPHI. The practice is required to establish and implement procedures to create or maintain retrievable, exact copies of EPHI that may be lost in the event of a security incident. The practice is also required to establish procedures to restore any loss of data — that is, the process that it will follow to ensure that the data is restored. In addition, the Practice is required to establish procedures to enable communications of critical business processes for the protection and security of EPHI while operating in emergency mode.

An important step in maintaining the integrity of your electronic protected health information is implementing backup policies and procedures. Each employee should be aware of the importance of this activity and how their actions can impact the practice.

A backup is a duplication of data that is stored on the server and/or workstation. The purpose is to be able to retrieve any information that might have been lost or destroyed for whatever reason (e.g., virus, power failure, equipment failure, user error, etc.). As a result of these various vulnerabilities, data may be rendered useless or lost. The creation of backups thus ensures that any redundant data of the practice can be restored quickly in the event that parts of the operative data are lost. The loss of stored data can have a substantial adverse effect on a practice. The loss of application data or patient databases could threaten the existence of a private practice.

To Do

- Fill in your practice name on Exhibit 8.
- Determine who will perform backups and restorations. Will this be your Security Official or his/her designee?
- Determine what your current applications and system is capable of performing.

• Determine what you will backup.

• Determine what media you will use to back up your data (e.g., tape, CD, DVD, thumb drive, etc.).

• Determine how often you will backup (e.g., daily, twice a day, monthly, etc.).

• Determine how you will label your backup.

• Determine where you will store your backups (e.g., while in the office in protective box, off-site with Security Official, off-site in security deposit box at a financial institution, etc.).

• Determine how you will restore your data.

Stored data can be lost for a variety of reasons:

• Unsuitable environmental conditions (temperature, air moisture).

• Interference of magnetic data media by outside magnetic field.

• Destruction of data media (fire, water, vandalism)

• Inadvertent deletion or overwriting of files.

• Technical failure of external storage.

• Faulty data media.

• Uncontrolled changes and stored data (loss of integrity).

• Deliberate deletion of files with a computer virus.

The workforce must be knowledgeable of the features that save data. They vary with applications.

• Some programs auto save once “Enter” is selected/pressed.

• Other programs require a specific request to either “Save” or ”Save As.” Your workforce should understand that saving their work is the first step in maintaining EPHI.

• Store backups off-site. The Security Official or their designee should store the backup off-site in a fireproof container at the end of each business day.

Just as important as backing up data is the restoration of previously backed-up data. The restoration of data using data backups must be tested at regular intervals, at least after every modification to the data backup procedure. Consistent testing by the practice will ensure that:

- Data restoration is possible.
- The data backup procedure is practical.

- There is sufficient documentation of the data backup, thus allowing a substitute to carry out the data restoration, if necessary.

- The time required for the data restoration meets the availability requirements.

Finally, and most important is the storing of the practice‘s backup. It is recommended that backups be stored off-site. Backups should be stored in a fireproof box when in the office, but at the end of the business day, the backup should be removed to a secure off-site location by the Security Official or their designee.

Step 12: Develop Security Incident Policies and Procedures

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	**Required vs. Addressable**
Administrative	Security Incident Procedure	Response and Reporting	Required

See Exhibit 9: Sample Security Incident Policy & Procedures.

See Exhibit 10: Sample Security Incident Log.

As hard as a practice may try to prevent unauthorized entry into its computer system, there are instances that will occur where the practice's computer system is either intentionally or unintentionally accessed. There are individuals who will intentionally attempt to disrupt the practice's operations by utilizing techniques to gain access to the practice's computer system for personal gain. The practice is required to report internally and respond to security incidents, mitigate the harmful effects, and to document such incidents as well as the practice's response(s).

Regardless of whether these incidents are intended or accidental, the practice is required to have policies and procedures in place to identify, handle, and correct such incidents. The inability to respond to such incidents heightens the practice's vulnerability and potentially makes it easier for incidents to occur in the future. The practice needs to consider physical access to the practice and the computer system and its components as well as preventing unauthorized access to EPHI.

To Do

- Designate an individual in the practice to develop, implement, and monitor security incident policies and procedures.
- Create and maintain a log of security incidents regardless of intention. (See Exhibit 10).
- Develop policies and procedures to track and respond to security incidents. (See Exhibit 9).

Note

Types of computer security incidents that may occur (and are required to be reported and documented internally) include the following:

- Incidents involving computer "hackers" or unauthorized individuals who attempt to access the computer system by guessing User IDs and passwords to gain access to the practice's computer system;
- Incidents involving malicious computer codes, such as viruses (See Step 9);

- Unauthorized access to the practice, such as through obtaining a key to the practice‘s office space without authorization and utilizing it to enter the practice;
- Unauthorized use and distribution of confidential practice information, including PHI and EPHI;
- Use of the practice‘s computer to commit illegal acts; and
- Unauthorized use, destruction, alteration, or theft of the practice‘s computer hardware and software equipment

Step 13: Implement Facility Maintenance Log

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	**Required vs. Addressable**
Physical	Facility Access Controls	Maintenance Records	Addressable

See Exhibit 11: Facility Maintenance Log.

The Security Rule includes a standard to implement policies and procedures to limit physical access to its electronic information systems, while ensuring that proper access is allowed. In order to satisfy the Facility Access Controls requirement, practices must address whether or not it is reasonable and appropriate to implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks). Exhibit 11 provides an appropriate form of maintenance log for use in compliance with this particular implementation specification.

To Do

- Fill in practice name on Exhibit 11.
- File in your Security Manual folder.
- Use when items that affect your practice‘s physical security are in need of repair.

Note

- It is reasonable and appropriate for practices of all sizes to document repairs and modifications to their facility.
- The log is a means to keep the practice aware of their security issues.
- It is important to keep the log up to date.
- Based on facility changes, security policies and procedures may need to be revised.
- Train staff if revisions are made to the security policies and procedures.

Step 14: Develop Facility Security and Contingency Plans

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	**Required vs. Addressable**
Administrative	Contingency Plan	Data Backup Plan	Required
Administrative	Contingency Plan	Disaster Recovery Plan	Required
Administrative	Contingency Plan	Emergency Mode Operation Plan	Required
Administrative	Contingency Plan	Testing and Revision??	Addressable
Administrative	Contingency Plan	Applications and Data Criticality Analysis	Addressable
Administrative	Security Management Process	Risk Management	Required
Physical	Facility Access Controls	Contingency Operations	Addressable
Physical	Facility Access Controls	Facility Security Plan	Addressable

See Exhibit 12: Sample Contingency Policy & Procedure.

See Exhibit 13: Contingency Plan Steps.

A contingency plan protects the availability, integrity, and security of data during unexpected negative events (e.g., floods, fires, or terrorism). The Security Rule requires practices to establish and implement policies and procedures for responding to an emergency that damages systems that contain EPHI. The policies and procedures should address information systems (See Step 11) as well as the practice's brick and mortar facility(ies). This applies to practices that are located within a medical complex, as well as in their own, wholly occupied, stand-alone building.

Although many threats and vulnerabilities cannot be avoided, some threats can be prevented or at least anticipated. Therefore, it is important that practices assess their facilities internally and externally as a means of preemptive preparation.

To Do

- Assess the practice's risks. Practices will need to assess their risks annually if not quarterly.
- Highlight those issues that need to be addressed immediately.
- Determine which issues constitute Contingency Plans.
- Implement Contingency Policy and Procedure. (Exhibits 12 and 13)

Note

• The Security Rule **requires** practices to periodically audit and access their Contingency and Security Plans.

• It is important that the Steps to Activate a Contingency Plan be addressed during the planning stages and not only when a contingency plan needs to be activated.

The primary focus of a contingency plan revolves around the protection of the practice's electronic protected health information. The contingency plan should address the protection, safety, and recovery of data.

Note

There are three types of threats that a practice should address:

1. Natural (e.g., tornado, hurricane, earthquake, flood, fire, etc.).
2. Human (e.g., introduction of viruses, sabotage, operator error, vandalism, terrorism, etc.).
3. Environmental (e.g., hardware failure, software failure, network failure, power failure, etc.).

In addition to considering the three types of threats, a practice should consider emergent versus non-emergent threats when creating their contingency plans. Examples of non-emergent threats would be forecasted weather and planned power outages.

Practices need to determine which of these threats are applicable to their circumstances and implement contingency plans in order to prevent a disaster or emergency situation from happening and, as appropriate, respond effectively in the event of such a disaster or emergency. An effective contingency plan will be applicable, feasible, and effective at restoring EPHI.

Note

Practices should **consider** being equipped with or having on hand:

• UPS (Uninterruptable power supplies) to provide short-term backup power.
• Generators to provide long-term backup power.
• Fire extinguishers.
• Fire and smoke detectors.
• Water sensors on server room floor and ceiling.
• Fire and waterproof containers for backup storage off site.
• Sufficient backup media.
• AM/FM Radio with battery.

Practices need to determine to what extent they will design their Contingency Plan. All three types of threats (i.e., natural, human, and environmental) need to be taken into consideration, however, practices can either incorporate their responses or create individual plans per threat.

Step 15: Develop a List of Business Associates and Implement Agreements

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	Required vs. Addressable
Administrative	Business Associate Agreements and Other Arrangements	Written Contract of Other Arrangement	Required

See Exhibit 14: Listing of Typical Business Associates.

See Exhibit 15: A Medical Practice Guide for the Security Official to Identify Business Associates that Access PHI. (This exhibit need only be viewed by the Security Official or Physicians.)

See Exhibit 16: Business Associate Agreement.

The concept of a Business Associate was introduced in the Privacy Rule. Most medical practices require the assistance of other businesses and contractors to carry out their day-to-day operational activities. In general (and for purposes of the Security Rule), a Business Associate is any person or entity that creates, receives, maintains, or transmits electronic protected health information on behalf of the practice and is not a part of the practice's workforce.

Under the Security Rule, practices must enter into business associate agreements with persons or entities who meet the definition of a business associate. The agreements must contain satisfactory assurances from the business associate that it will appropriately safeguard the EPHI that it is granted access to in order to perform services for or on behalf of the practice.

WHAT IS A BUSINESS ASSOCIATE?

A business associate is a person or entity that creates, receives, maintains, or transmits protected health information to carry out certain functions or activities on behalf of the practice and is not a part of the practice's workforce.

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, keeps 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.

The determination of who is or is not a business associate is likely to vary from situation to situation. It is important to note the difference in the Privacy Rule and the Security Rule at this point. The Security Rule solely addresses protected health information that is created, received, maintained, or transmitted in electronic form. The Privacy Rule, on the other hand, also includes verbal and written (non-electronic) communication.

Similar to the Privacy Rule, in some situations, covered entities may be a business associate 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.

If your business relationships with your business associates involve the use or disclosure of EPHI, your practice will need to ensure that its current business associate agreements include language that satisfies the requirements of the Security Rule.

If the practice does not have a business associate agreement in place, it is appropriate to use the complete form of business associate contract set forth in the HIPAA Privacy Manual.

Exhibit 14 lists some "typical" Business Associates under the Security Rule. 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 15 to determine on a case-by-case basis if a person or entity is a Business Associate with whom you need to execute a contract.

Ensure that all Business Associate Agreements are in place:

• Fill in Practice Name on Exhibit 16.

• Security Official should compile a list of Business Associates, using Exhibits 14 and 15, and any list of Business Associates that you have previously compiled. 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. 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 15 for each person or entity.

• 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 should 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.

• Some Business Associates may present you with their own version of a Business Associate Agreement. 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 Contract.

•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.

• 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 and accordingly, needs a Business Associate Agreement with the practice.

•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.**

It is recommended that legal counsel review the model contract or amendment, as may be the case, prior to use by the practice.

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).

Step 16: Create Computer Workstation Use Policies and Procedures

Step 16:

Create Computer Workstation Use Policies and Procedures

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	**Required vs. Addressable**
Physical	Workstation Use	None	Required
Physical	Workstation Security	None	Required

See Exhibit 17: Sample Policy and Procedures on Workstation Use.

The Security Rule requires practices to establish policies and procedures regarding the secure use of workstations. The practice must implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access EPHI. In addition, the practice must implement physical safeguards that restrict access to unauthorized users from all workstations that access EPHI.

It is important to note that the definition of workstation encompasses more than just a desktop PC. A workstation can also be a laptop computer, tablet or smartphone.

WHAT IS A WORKSTATION?
A **Workstation** is a computer used for running software applications, storing, and transmitting data. In networking, workstation refers to any computer connected to a local area network. In a medical practice, workstation refers to any computer, terminal or other device that allows access to the practice's data.

To Do

- Fill in the practice name on Exhibit 17.
- Identify the proper functions to be performed at each workstation.
- Identify the manner in which the functions are to be performed.
- Review the physical attributes surrounding the workstations.
- Identify the specific systems that may be used to access EPHI (on-site and off-site).
- Customize Exhibit 17 to suit the needs of your practice.

Note

NEED TO ADDRESS:

- What types of workstations are used (e.g., desktop, portable, tablets, smartphones)?
- What are the environmental issues that need to be addressed?
    1. Surge protectors
    2. Food and beverage
    3. Virus scanning
    4. Media use (e.g., CD, DVD, thumb drive)
- Distributions of User Ids and Passwords (See Step 6)
- Automatic log off procedures (See Step 7)
- Printers
- Email
- Internet Access
- Remote Access
- Access by Business Associates (See Step 15)
- Backup Procedures (See Step 11)
- Sanctions (See Exhibit 23)

Note

Not all practices will need to address everything on the Need to Address list. The Security Rule is flexible to your needs.

Step 17: Document and Train All Physicians and Staff on the Security Policies and Procedures

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	**Required vs. Addressable**
Administrative	Workforce Security	Workforce Clearance Procedures	Addressable
Administrative	Information Access Management	Access Authorization	Addressable
Physical Administrative	Security Awareness Training	Security Reminders Password Management	Addressable Addressable

See Exhibit 18: Security Policy Training Checklist.

See Exhibit 19: Training Documentation Form.

All physicians and staff (your workforce) must be trained on the practice's Security Policies and Procedures and how they affect their individual job responsibilities. Your Security Policy Training Checklist is provided in Exhibit 18 to assist your Security Official in conducting the Security training.

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

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

- Fill in Practice Name on Exhibits 18 and 19.
- Photocopy the Security Policy Training Checklist and Training Documentation Form as needed for each training session conducted.
- After the training session, have physicians and staff record their names, titles, and signatures on the Training Documentation Form.
- The Security Official should maintain the Training Documentation Form(s).
- The Security Official 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 in the event of confusion or questions regarding the Security Policies.

- Modify the new employee orientation checklist to include time set aside for Security Policy training and to make certain that the employee has signed the Training Documentation Form.

- All new employees must receive security training as a part of their initial employee orientation.

- Any time there is a material change in the Security Policy that affects your practice and how your staff conducts business; the employees whose functions and responsibilities are affected by the change must receive additional training.

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

- The Security Rule includes a specification that practices implement periodic security reminders once training has been accomplished. This component is addressable allowing practices to determine how best to accomplish this step for their practice (e.g., weekly meetings, emails, etc.).

Step 18: Obtain Signed Workforce Confidentiality Agreements from All Physicians and Staff

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	**Required vs. Addressable**
Administrative	Workforce Security	Workforce Clearance	Addressable
Administrative	Information Access Management	Authorization and/or Supervision Access Management	Addressable Addressable
Physical Administrative	Security Awareness and Training	Security Reminders Password Management	Addressable

See Exhibit 20: Workforce Confidentiality Agreement.

Although the Security Rule does not require employees to sign a confidentiality agreement, the Rule does require a practice to implement policies and procedures relating to the regulation, access, and use of EPHI by members of its workforce. Further, the Rule does require a practice to train its workforce members regarding such policies and procedures.

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

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

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 Security Official.
- 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.

Note

• If you have already implemented Workforce Confidentiality Agreements as a part of your current policies and procedures, you will want to make sure that they include appropriate security measures based on this Security Manual, and if not, update them to do so.

• Exhibit 20 addresses both Privacy and Security.

Note

• 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.

• If 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.

Step 19: Monitor Compliance with the Security Rule

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	**Required vs. Addressable**
Administrative	Security Management Process	Risk Management Information System Activity Review	Required Required
Administrative	Information Access Management Security Awareness and Training	Security Reminders	Addressable Addressable
Administrative	Evaluation	None	Required

The Security Rule requires the practice to consistently monitor its compliance efforts and update its policies, procedures, and systems accordingly. The Security Official has the responsibility to monitor the practice's compliance with the Security Rule. The Security Official should encourage all physicians and staff to communicate openly with him/her concerning any potential security breaches and to provide recommendations for how the practice could be better organized to protect patient's EPHI. Note that no physician, provider, or staff member is exempt from adhering to the Security Rule.

If staff members are aware of a possible violation of the Security Rule that involves the Security Official, then they should be encouraged to communicate directly with the president of the practice or another individual who is in an executive leadership position.

The practice 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 not a breach is. The following are not considered breaches:

- 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;

- 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

- 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:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- 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."

See the **American Psychiatric Association's** Privacy Manual for additional details about HIPAA's breach notification requirements.

Example of an Event Record:

Event Type	Time and Date Event Occurred	User ID Associated with the	Computer System Component	Follow Up
Employee who was not authorized to access the billing system	4:00 p.m. on 4/4/2013	S. Jones	Billing Software	Meeting with S. Jones regarding unauthorized access. Verbal warning. Understanding will receive written warning if it happens again.

Note

• The Security Official should create processes to monitor compliance

• The Security Official should offer a mechanism by which staff can address Security concerns without the risk of repercussions to themselves.

• An Event Log or sufficient similar documentation should be maintained by the Security Official to record the receipt of complaints. The log should include the follow-up on all Security complaints.

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

• Appropriate measures need to be taken by the Security Official to prevent repeat violations or potential violations of the Security Rule.

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

• The practice is required to mitigate or reduce any harmful effects known to the practice regarding an unauthorized use of or access to EPHI in violation of the Security Rule or the practice‘s Security Policies and Procedures.

Step 20: Evaluate All Policies and Procedures Periodically

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	**Required vs. Addressable**
Administrative	Evaluation	None	Required

The Security Rule **requires** that practices regularly evaluate their compliance with the Security Rule. The evaluation must consider technical and non-technical components of the Rule's requirements. Some measures may be addressed daily, such as the data backup process. Some measures may be addressed weekly, such as the audit trails or general availability of authorized access to the information system. Still, other measures may be addressed annually, such as repeating the Risk Analysis and Contingency Plan Steps.

To Do

- Determine which processes you will review.
- Determine frequency of review (e.g., backup daily, audit trail weekly, risk assessments quarterly, etc.).
- Make sure you have made a master copy of the Risk Analysis (Exhibit 2).

Note

- It is just as important to review your security policies following system changes and procedures as it is following a report of a security incident. The Security Rule requires such reviews in response to any changes that affect the security of EPHI.

Step 21: Create Workforce Termination Procedures

Snapshot Compliance Components			
Safeguard	**Standard**	**Implementation**	**Require vs. Addressable**
Administrative	Workforce Security	Termination Procedure	Addressable

See Exhibit 21: Sample Workforce Termination Procedures.

See Exhibit 22: Workforce Termination Checklist.

The Security Rule includes a standard to implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI. One of the implementation specifications within that standard is termination procedures. Practices must address whether it is appropriate and reasonable to implement a procedure for termination of access to PHI, including EPHI, when an employee is either terminated or leaves voluntarily.

It is recommended that the practice have procedures in place to protect access to the practice's physical and computer assets in the event that an employee or other member of the practice is terminated or leaves the practice voluntarily. The Security Official or his/her designee should implement these procedures immediately after an individual's employment or affiliation with the practice is terminated.

To Do

- Fill in practice name on Exhibits 21 and 22.
- Create workforce termination procedures. See Exhibit 21 for sample procedures.
- Create workforce termination procedures checklist to document that all necessary items are handled upon termination of an individual's employment or affiliation with the practice. See Exhibit 22 for a sample checklist.
- Familiarize yourself with the procedures and checklist and be ready to implement if/when necessary.
- Workforce termination policies should be implemented regardless of the circumstances under which an individual leaves the practice.
- Under "friendly" terms:
- Discuss responsibilities for keeping certain information confidential and private.
- Determine if the employee should clean out his/her hard drive prior to his/her departure.
- Under "unfriendly" or adverse terms:
- Revoke his/her access to the computer system as soon as possible.

• If the employee is fired, access should be revoked just before or at the same time he/she is notified of his/her dismissal.

• Under “friendly” and “unfriendly” terms:

• Employee‘s physical access to the practice – keys, facility passcards, alarm codes, and ID badges should be collected prior to the employee‘s departure.

• Consider all workforce members who may have access to the physical office and computer system, (e.g., temporary employees, practice volunteers, and part-time employees).

• In addition to the practice‘s obligations under the Security Rule, the practice must be mindful of and adhere to applicable federal and state employment laws and should seek the advice of legal counsel when questions or risks arise, prior to terminating a member of the workforce.

Step 22: Implement Sanction Policy

See Exhibit 23: Sample Sanction Policy.

Practices are **required** to implement a sanction policy in order to hold members of their workforce and Business Associates accountable to the practice's security policies. Exhibit 23 is a sample sanction policy that practices may use as a guide.

It is important that your sanction policy be written specific to your practice's specific needs, expectations, and obligations. The sample policy provided addresses the following points: Determine if practice will use the sample Sanction policy provided (see Exhibit 23) and if so fill in the Practice name on Exhibit 23. If not, practices may customize Exhibit 23 to best suit their practice needs.

To Do

- State why the sanction policy has been adopted.
- State why the Security Policy has been adopted.
- Outline what steps to take if someone believes the Security Policies have been violated.
- Explain the steps the Security Official will take to investigate an incident.
- Outline what type of disciplinary actions will take place.
- Inform of possible criminal implications.
- Inform of possible ethical implications.
- Include an "at-will employment" statement, if applicable to your state.
- Specifically state that every member of the workforce is expected to comply.

Practices will want to specify their disciplinary measures if their situation does not warrant the use of the extensive sample sanction policy (Exhibit 23) included in the manual. The sample policy can be altered to suit a practice's specific requirements. The Security Rule does not require specific language; only that a sanction policy is put into place. Practices only want to include those measures that they plan to enforce and should be aware that the HIPAA Security Rule will most likely not pre-empt the Practice's obligations under applicable federal and state employment laws.

Exhibit 1: Security Official Job Responsibilities

Security Official Job Responsibilities

_____
Insert Practice Name

The Security Official 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 security of patients‘ electronic protected health information (EPHI) in compliance with federal and state laws and the practice‘s security policies and procedures (the ”Security Policy”).

Responsibilities:

Maintains the confidentiality, integrity, and availability of patient’s EPHI.

Maintain current knowledge of applicable federal and state security laws.

Develop, oversee, and monitor implementation of the practice‘s Security Policy and ensure that the integrity of the Security Policies is maintained at all times.

Report regularly to the practice governing body and officers and/or owners (as applicable) regarding the status of the Security Policies.

Work with legal counsel, consultants, management, and committees to ensure that the practice maintains appropriate 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 security policies and procedures in coordination and collaboration with other similar functions, and, when necessary, with legal counsel.

Oversee, direct, deliver, or ensure the delivery of security training and orientation to all employees, volunteers, medical and professional staff, and other appropriate personnel (practice workforce).

Monitor attendance at all Security Policies training sessions and evaluate participant’s comprehension of the information provided at training sessions as well as maintain appropriate documentation of security training.

Monitor practice compliance with Security Policies including periodic security risk assessments.

Monitor and evaluate, on no less than an annual basis, the Security Policies success in meeting the practice‘s goal for protection of EPHI.

Coordinate and participate in disciplinary actions related to the failure of practice workforce members to comply with the practice‘s Security Policies and/or applicable law.

Monitor access controls to EPHI. Maintain access to EPHI only by authorized personnel.

Monitor technological advancements related to electronic protected health information protection and security 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 Security Policies.

Initiate, facilitate, and promote activities to foster security information awareness within the practice.

Cooperate with OCR, other legal entities, and practice officers or owners 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 the practice‘s legal counsel in an ongoing manner and in the event of a reported violation.

Collaborate and coordinate with the practice’s Privacy Official regarding the appropriate breach notification response and the performance of a risk assessment.

Maintain all business associate agreements and respond appropriately if problems arise.

Act as the practice-based point of contact for receiving, documenting, and tracking all complaints concerning security policies and procedures of the practice.

Maintain documentation of the practice‘s Security Policies and Procedures for a minimum of six years from the date the practice created the policies and procedures or last updated the policies and procedures.

Responsible for overseeing the maintenance of the practice‘s hardware and software.

Accountable for tracking hardware and software inventory.

Responsible for overseeing the installation and connectivity of computer equipment.

Responsible for monitoring daily, weekly, and monthly backup procedures.

Responsible for disposal and media re-use.

Skills:

Able to facilitate change.

Possess knowledge and understanding of federal and state security laws and of the medical practice‘s information technology.

Exhibit 1A: Privacy & Security Official Job Responsibilities

Privacy & Security Official Job Responsibilities

_____
Insert Practice Name

The Privacy & Security Official 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 and security of patients' protected health information (PHI) in compliance with federal and state laws and the practice's privacy and security policies and procedures.

Responsibilities:

Maintain the confidentiality, integrity, and availability of patient's PHI.

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

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

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

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 and security 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, restrict the means of communication, or 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 (practice workforce) and maintain appropriate documentation of privacy training.

Monitor attendance at all Privacy and Security Policies training sessions and evaluate participant's comprehension of the information provided at training sessions.

Monitor compliance with Privacy and Security Policies including periodic privacy risk assessments.

Monitor and evaluate, on no less than an annual basis, the Privacy and Security Policies' 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's Privacy and Security Policies and/or applicable law.

Monitor access controls to EPHI. Maintain access to EPHI only by authorized personnel.

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 and Security Policies.

Initiate, facilitate, and promote activities to foster privacy and security information awareness within the practice.

Cooperate with the OCR, HHS, other legal entities, and practice officers or owners 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's legal counsel in an ongoing manner and in the event of a reported violation.

Investigate all reported breaches of PHI and perform the risk assessment and make any required breach notifications.

Maintain all business associate agreements and respond appropriately if problems arise.

Act as the practice-based point of contact for receiving, documenting, and tracking all complaints concerning privacy and security policies and procedures of the practice.

Maintain documentation of the practice's security policies and procedures for a minimum of six years from the date the practice created the policies and procedures or last updated the policies and procedures.

Responsible for overseeing the maintenance of the practice's hardware and software.

Accountable for tracking hardware and software inventory.

Responsible for overseeing the installation and connectivity of computer equipment.

Responsible for monitoring daily, weekly, and monthly backup procedures.

Responsible for disposal and media reuse.

Skills:

Able to facilitate change.

Possess knowledge and understanding of federal and state privacy security laws of the medical practice‘s information technology.

Exhibit 2: HIPAA Security Rule Standards Matrix and Risk Analysis

HIPAA Security Rule Standards Matrix and Risk Analysis

_____

Insert Practice Name

_____

Date

This matrix is to be used to satisfy the **required** risk assessments of the practice. Practices should keep a master copy of the matrix for future assessments. The HIPAA Security Rule requires practices to conduct an **initial risk analysis** to identify the potential vulnerabilities to the confidentiality, integrity, and availability of EPHI. Thereafter, practices are required to reassess in response to any environmental or operational changes related to the protection of their EPHI.

The first column provides reference to the standards and implementation specifications within the Rule. Column two (2), **Guidelines for Compliance and Reviewable Procedures**, provides questions for the practice to answer in order to help them assess and reassess risk. Practices should document their answers in this column (e.g., yes or no). Columns three (3) & four (4) are reference columns that define the Steps within the manual that assist the practice in implementing each standard. Finally, Column five (5), **Actions**, provides the practice a place to document the actions that they took, based upon the questions from Column two (2), in order to implement the standards, either **required** or **addressable**.

Standard and Implementation Specifications

HIPAA Security Rule Standards Matrix and Risk Analysis

Guidelines for Compliance and Reviewable Procedures	Steps	Exhibits	Actions	Administrative Safeguards
Standard: Security Management Process §164.308(a)(1)				
Implement policies and procedures to prevent, detect, contain, and to correct security violations.	Has the practice ever conducted a security analysis of its network using a network-scanning program?	3, 4, 6, 22	2, 3	
Implementation Specifications: Risk Analysis – Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by the covered entity. **(Required)**	Has the practice evaluated its computer system(s) to verify that appropriate security measures are in place?			
Risk Management – Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Rule. **(Required)**	Based on the two (2) previous questions, if the security features in place are not adequate or there are no security features in place, has the practice identified and selected security features to implement?			
Sanction Policy – Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. **(Required)**	Does the practice have any custom programming on the system that was not created by the original vendor?			

HIPAA Security Rule Standards Matrix and Risk Analysis (continued)

Standard and Implementation Specifications	Guidelines for Compliance and Reviewable Procedures	Steps	Exhibits	Actions
Information System Activity Review – Implement procedures to regularly review records of information systems activity, such as audit logs, access reports, and security incident tracking reports. §164.308(a)(1) (ii) (A-D) (Required)	Does the practice have a written security policy that describes the practice's plans, procedures, and sanctions with respect to all security components of its EPHI related computer systems? If so, where is the policy form in the manual? Has the practice tested its computer system to determine that the appropriate security features are working correctly and are adequate for the practice's computer system? Does the practice guard data integrity, confidentiality, and availability by access control, audit control, authorization control, and data authentication? Is there a regular audit of the practice's computer system records?	4, 6, 16, 20, 22	1, 3, 5, 23	
Standard: Assigned Security Responsibility §164.308(a)(2) Identify the security official who is responsible for the development and implementation of the policies and procedures required by the Security Rule. (Required)	Does the practice have a job description for the Security Official? Who is the designated Security Official?	2	1, 1A	

HIPAA Security Rule Standards Matrix and Risk Analysis (continued)

Implementation Specifications	Guidelines for Compliance and Reviewable Procedures	Steps	Exhibits	Actions
Standard: Workforce Security §164.308(a)(3)(i) Implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI, as provided under this section, and to prevent those workforce members who do not have access under this section from obtaining access to EPHI.	Does the practice provide security training to all employees and providers? Does the practice have a designated staff member or vendor(s) who handles problems and issues with hardware and software, access to and maintenance of servers, software training, and technical problems with the practice's workstations?	2, 5, 8, 21	1, 1A, 21, 22	
Implementation Specifications: Authorization and/or Supervision – Implementation procedures for the authorization and/or supervision of workforce members who work with EPHI or locations where it might be accessed **(Addressable)**	Do temporary employees have access to the system? Are there different levels of security assigned to different staff members depending on their job responsibilities? Does the practice use an outside transcription service?			
Workforce Clearance Procedures – Implement procedures to determine that the access of a workforce member to EPHI is appropriate. **(Addressable)**				
Termination Procedures – Implement procedures for termination of access to EPHI when the employment of a workforce member ends or as required by determinations made as specified by the Administrative Safeguards section of the Security Rule. **(Addressable)** §164.308(a)(3)(ii) (A-C)	Does the practice have formal, documented instructions to ensure that terminated employees or other users, including temporary employees, no longer have access to confidential data? For example, are passwords terminated, keys and keycards returned immediately upon termination of employment?			

HIPAA Security Rule Standards Matrix and Risk Analysis (continued)

Standard and Implementation Specifications	Guidelines for Compliance and Reviewable Procedures	Steps	Exhibits	Actions
Standard: Information Access Management §164.308(a)(4)(i) Implement policies and procedures for authorizing access to EPHI that are consistent with the applicable requirement of the Privacy Rule. **Implementation Specifications:** Access Authorization – Implement policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, process, or other mechanism**. (Addressable)** Access Establishment and Modification – Implement policies and procedures that, based upon the entities accessed authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. **(Addressable)** §164.308(a)(4)(ii)(B-C)	Does the practice utilize biometrics, passwords, personal identification numbers, or telephone callback procedures to verify authorized users? Does the practice restrict testing and revision of physical access controls to authorized personnel? Does the practice have a designated staff member or vendor(s) who loads software applications or upgrades onto the PC? Is the network used for file sharing (e.g., between staff members and physicians)? Are passwords given out to non-employees (e.g., pharmaceutical representatives, insurance companies)? Does the practice allow dial up or other remote access to the system (e.g., from home, such as using PC Anywhere or Citrix, or using direct access)? If so, does the practice have documented policies and procedures that establish the rules for granting access to EPHI, including how an employee or other party working on or near EPHI accesses it? Does the practice ensure that authorized individuals have physical access to information and unauthorized users do not? Does the practice have a process for modification of an entity's level of access to EPHI?	6, 8, 18	5, 17, 20	

HIPAA Security Rule Standards Matrix and Risk Analysis (continued)

Standard and Implementation Specifications	Guidelines for Compliance and Reviewable Procedures	Steps	Exhibits	Actions
Standard: Security Awareness and Training §164.308(a)(5)(i) Implement a security awareness and training program for all members of its workforce (including management). **Implementation Specifications:** Security Reminders – Periodic security updates. **(Addressable)** Protection from Malicious Software – Procedures for guarding against, detecting, and reporting malicious software. **(Addressable)** Log-In Monitoring – Procedures for monitoring log-in attempts and reporting discrepancies. **(Addressable)** Password Management – Procedures for creating changing, and safeguarding passwords. **(Addressable)** §164.308(a)(5)(ii)(A-D)	Are practices providing their workforce with periodic security updates and information reminders? Does the practice have software installed on its computer system(s) and workstations that checks for computer viruses? If so, does the practice have policies and procedures in place referencing the use of virus and firewall software? If policies are in place, how often are they reviewed? Is there a security measure that handles information downloads? Are there other methods of data download, such as Zip Drives or Read/Write CD ROMs? Does the practice access the Internet through the network? Does the practice have an Internet firewall? Are tracking features in place to monitor who is accessing the software? Does the practice monitor who is accessing the system via dial up connections? Does the practice maintain a log of who accesses the network? Does the practice maintain a record of which staff and physicians have accessed secure and confidential information?	6, 9, 12, 16, 18, 19, 21	1, 1A, 3, 6, 7, 9, 10, 17, 21, 22	

HIPAA Security Rule Standards Matrix and Risk Analysis (continued)

Standard and Implementation Specifications	Guidelines for Compliance and Reviewable Procedures	Steps	Exhibits	Actions
Password Management (cont'd)	Are there passwords to access the clinical management software? Are there procedures in place for accessing EPHI in an emergency? Do temporary employees share login names with each other and/or permanent employees? Does the practice allow for the password protecting of documents? Does the practice disable passwords and other security features if handhelds or laptops are lost or stolen? Is network access governed by passwords? Are passwords changed on a regular basis? Are the user lists regularly checked against the current list of employees?	6, 9, 12, 14, 16, 18, 19, 21	1, 1A, 3, 6, 7, 9, 10, 17, 21, 22	
Standard: Security Incident Procedures §164.308(a)(6)(i) Implement policies and procedures to address security incidents. **Implementation Specification:** Response and Reporting – Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. (Required) §164.308(a)(6)(ii)	Is the practice documenting security incidents and addressing future preventable measures?	12	7, 9, 10	

HIPAA Security Rule Standards Matrix and Risk Analysis (continued)

Standard and Implementation Specifications	Guidelines for Compliance and Reviewable Procedures	Steps	Exhibits	Actions
Standard: Contingency Plan §164.308(a)(7)(i) Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI. Implementation Specifications: Data Backup Plan – Establish and implement procedures to create or maintain retrievable exact copies of EPHI. (Required) Disaster Recovery Plan – Establish procedures to restore any loss of data. (Required) Testing and Revision Procedure – Implement procedures for periodic testing of and revision of contingency plans. (Addressable) Emergency Mode Operation Plan – Establish (and implement as needed) procedures to enable continuation of critical business processes for the protection of the security of EPHI while operating in emergency mode. (Required)	Does the practice or vendor routinely test the practice's computer system(s) and modify its contingency plan and/or emergency recovery plan (e.g., quarterly, semiannually, annually)? Does the practice routinely back up the server(s)? Is there a formal system for tracking the receipt, manipulation, storage, dissemination, transmission, and disposal of EPHI to ensure its security? Does the practice have a designated staff member or vendor(s) who conducts the backup? Are the backups stored off site? Is there a designated staff member or vendor(s) who can recover data from a backup? Does the practice routinely test the backup? Does the practice keep a log of the backups? Is there a disaster recovery plan in place to respond to computer system emergencies or failure?	11, 14, 16	8, 12, 13, 17	

HIPAA Security Rule Standards Matrix and Risk Analysis (continued)

Standard and Implementation Specifications	Guidelines for Compliance and Reviewable Procedures	Steps	Exhibits	Actions
Applications and Data Criticality Analysis – Assess the relative criticality of specific applications and data in support of other contingency plan components. **(Addressable)** §164.308(a)(7)(ii)(A-E)	Are practices testing their contingency plan routinely to ensure its applicability? Does the server(s) have an emergency power supply? Does the practice have measures in place to ensure the access to EPHI even while working in emergency mode? Do practices know which systems they consider to be critical to running their practice (e.g., practice management software, EMR, etc.)?	14	13	
Standard: Evaluation §164.308(a)(8) Perform periodic technical and non-technical evaluation, based initially upon the standards implemented under the Security Rule and subsequently, in response to environmental or operational changes affecting the security of EPHI, that establishes the extent to which the entity's security policies and procedures meet the requirement of the Security Rule. **(Required)**	Is there a regular audit of the practice's computer system records? Future Assessments: Have all policies and procedures been reviewed? How often are policies and procedures reviewed? Has the practice reviewed the questions in this column and verified that all previous answers either still apply or have changed. If they have changed, have the practice's actions to respond to those changes been documented?	4, 5	3	
Standard: Business Associate Agreements and other Arrangements §164.308(b)(1) **Implementation Specification:** Written Contract or Other Arrangement **(Required)** §164.308(b)(4)	Has the practice checked with all computer hardware vendors to ensure that routine changes (upgrades, testing, and maintenance) to the computer system do not compromise security? Does the practice have appropriate contracts in place for each business associate with whom it electronically shares EPHI?	1, 5	14, 15, 16	

HIPAA Security Rule Standards Matrix and Risk Analysis (continued)

Standard and Implementation Specifications	Guidelines for Compliance and Reviewable Procedures	Steps	Exhibits	Actions
Standard: Facility Access Controls §164.310(a)(1) Implement policies and procedures to limit physical access to its electronic information systems in the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. **Implementation Specifications:** Contingency Operations – Establish (and implement as needed) procedures that allow facility access in support of restoration of loss of data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. **(Addressable)** Facility Security Plan – Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft. **(Addressable)** Access Control and Validation Procedures – Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing or revision. **(Addressable)** Maintenance Records – Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). (Addressable) §164.310(a)(2)(i-iv)	**Physical Safeguards** Is there a contingency plan in place to respond to computer system emergencies and natural disasters (e.g., intrusion, theft, flooding, and fire)? Is the practice's computer server(s) onsite or off? If the practice has remote locations, does each remote site have its own server(s)? Does the practice or vendor(s) have a process in place to recover lost data from each workstation? Is the practice located in a medical complex or stand-alone facility? Does the practice have a plan to protect the exterior and interior of the practice and/or building from unauthorized physical access? Is there a Security Guard located at the facility? Does the practice sign-in and escort visitors when appropriate? Does the practice maintain a log of repairs and other modifications to the physical components of the office?	13, 14	11, 12, 13	

HIPAA Security Rule Standards Matrix and Risk Analysis (continued)

Standard and Implementation Specifications	Guidelines for Compliance and Reviewable Procedures	Steps	Exhibits	Actions
Standard: Workstation Use & Security §164.310(b-c) Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, the physical attributes of the surroundings of a specific workstations or class of workstation that can access EPHI and implement safeguards to restrict access to unauthorized users. **(Required)** **Standard: Device and Media Controls** –§164.310(d)(1) Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility and the movement of these items within the facility. **Implementation Specifications:** Disposal – Implement policies and procedures to address the final disposition of EPHI and/or the hardware or electronic media on which it is stored. **(Required)** Media Re-use - Implement procedures for removal of EPHI from electronic media before the media are made available for reuse**. (Required)** Accountability – Maintain a record of the movements of the hardware and electronic media and any person responsible therefore. **(Addressable)** Data Backup and Storage – Create a retrievable, exact copy of EPHI, when needed, before movement of the equipment**. (Addressable)** §164.310(d)(2)(i-iv)	Does the practice's staff share workstations (e.g., with each other or with temporary employees)? Does staff or providers remove software from the practice (e.g., thumb drives)? Are the laptops available for shared use? Does the practice use handheld computers (e.g. Blackberries, IPhones, iPads, etc.)? If so, do the handheld devices transmit or carry EPHI? Are the practice's workstations locked and secure? Does the practice have policies and procedures for handling the destruction of computerized patient records? Is there a formal system for tracking the receipt, manipulation, storage, dissemination, transmission, and disposal of EPHI to ensure its security? Does the practice have policies and procedures in place for bringing hardware and software into and out of the practice? Does the practice have processes to ensure that EPHI has not been altered or destroyed by an unauthorized entity? Does the practice have formal, documented procedures for connecting new computer equipment and loading new computer programs? Does the practice re-use disks, tapes, drives, CDs, etc.? Does the practice periodically review and formally document maintenance performed on computer hardware and software?	16, 18 12, 13, 18	17, 20 1, 1A, 7, 20	

HIPAA Security Rule Standards Matrix and Risk Analysis (continued)

Standard and Implementation Specifications	Guidelines for Compliance and Reviewable Procedures	Steps	Exhibits	Actions
Data Backup and Storage	Does the practice maintain a log of repairs and other modifications to the physical components of the office? Does the practice keep an inventory of its workstations (i.e. hardware and software)? Is staff allowed to bring devices from home to attach to the workstations (e.g., laptops, tablets, handhelds)? Does the practice or vendor(s) perform routine backups of data on each workstation?	12, 13, 18	1, 1A, 7, 20	

Technical Safeguards				
Standard: Access Control §164.312(a)(1) Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access or rights as specified in the Security Rule. **Implementation Specifications:** Unique User Identification – Assign a unique name and/or number for identifying and tracking user identity. **(Required)** Emergency Access Procedure – Establish (and implement as needed) procedures for obtaining necessary EPHI during an emergency. **(Required)** Automatic Log-off - Implement electronic procedures that terminate electronic session after predetermined time of inactivity. **(Addressable)** §164.312(a)(2)(iii) Encryption and Decryption – Implement a mechanism to encrypt and decrypt EPHI. **(Addressable)** §164.312(a)(2)(i-iv)	Has the practice assigned a unique user identifier to each employee? Does the practice minimize the amount of access personnel has via procedures designed to limit access? Is the practice able to access EPHI in an emergency, such as with a universal or master User I.D. and password? Does the practice's computer system automatically log-off if it has not been used for a certain period of time? If so, is the practice using auto log-off technology or password protected screensavers? Does the practice transmit EPHI over a communications network? If so, does the practice use technology to ensure that a message received matches the message sent?	6, 7, 8, 18	5	

HIPAA Security Rule Standards Matrix and Risk Analysis (continued)

Standard and Implementation Specifications	Guidelines for Compliance and Reviewable Procedures	Steps	Exhibits	Actions
Standard: Audit Controls §164.312(b) Implement, hardware, software, and/or procedural mechanisms that record and examine activity and information systems that contain or use EPHI**. (Required)**	Can the practice account for all activity taking place with regard to their EPHI? (e.g., adding/removing of software/hardware, passwords, access, security incidents, etc.)	4, 6	3	
Standard: Integrity §164.312(c)(1) Implement policies and procedures to protect EPHI improper alteration or destruction.	Does the practice have procedures in place that protect EPHI from being altered or destroyed?	5, 8, 18	3, 5, 17	
Implementation Specification: Mechanism to Authenticate Electronic Protected Health Information – Implement electronic mechanisms to collaborate that EPHI has not been altered or destroyed in an unauthorized manner. **(Addressable)** §164.312(c)(2)				
Standard: Person or Entity Authentication §164.312(d) Implement procedures to verify that a person or entity seeking access to EPHI is the one claimed. **(Required)**	Do the computers, including handhelds, have built-in security features (e.g., passwords, encryption, automatic screen savers)?	8	5	
Standard: Transmission Security §164.312(e)(1) Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.	Is the server(s) accessible through modem connections?			
	Does the practice operate a Local Area Network (LAN)?	8		
Implementation Specifications: Integrity Controls – Implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of. **(Addressable)**	Does the practice operate a Wide Area Network (WAN)?			
	Does the practice use a Virtual Private Network (VPN) or a Value Added Network (VAN)?			
	Does the practice operate over a Wi-Fi connection?			
Encryption – Implement a mechanism to encrypt EPHI whenever it is	Does the practice employ encryption technology to protect			

deemed appropriate. **(Addressable)** §164.312(e)(2)(i-ii)	information from unintended parties? Does the practice have fax capabilities directly from their computers? If the practice is using encryption software, what are they using?			

Exhibit 3: Sample Audit Trails Policy and Procedures

Sample Audit Trails Policy and Procedures

_____
Insert Practice Name

Policy:

It is [Insert Practice Name's] policy to conduct audit trails to regularly track the identification and authentication of those accessing the computer system and to maintain records of the activity performed within the computer system.

Procedures:

The practice will designate an individual who will be responsible for implementing and adhering to the practice's audit trail policies and procedures. In addition to determining how to identify abnormal computer system activity through audit trails, the designated individual will also want to learn how to and familiarize himself/herself with normal computer system activity.

The practice will control access to audit logs and permit access to authorized individuals only. The practice must periodically monitor user activity, including password activity, to include when passwords are changed, who changed them, and when access privileges to software were changed and who changed them.

Audit trail reports must be generated and reviewed weekly. The audit trail reports must be kept in a secure location and retained for three years. Any abnormalities must be documented and immediately followed up on. Abnormalities include suspicious log-in attempts, unusually frequent password changes, and computer file changes and/or deletions.

The practice will create and maintain audit trail event records and keep these event records on file for a minimum of six months.

Exhibit 4: Sample Event Record

Sample Event Record

_____

Insert Practice Name

Event Type	Time and Date Event Occurred	User ID Associated with the Event	Computer System Component Involved	Follow Up
Employee who was not authorized to access the billing system	4:00 p.m. on 4/4/2013	S. Jones	Billing software	Meeting with S. jones regarding unauthorized access. Verbal warning. Understands will receive written warning if happens again.

Exhibit 5: Sample Policy for User Identification (User ID) and Authentication

Sample Policy for User Identification (User ID) and Authentication

_____
Insert Practice Name

Security Policy:

Access is the ability to interact with a computer system (e.g., use, change, or view). Users of the [Insert Practice Name] computer system must have access to certain information in order to adequately perform their assigned duties, pursuant to their individual job description.

[Insert Practice Name] uses user IDs and unique passwords to control access to [Insert Practice Name's] computer system. [Insert Practice Name] expects practice information to be available when it is needed, to be accurate, and to be safeguarded from access by unauthorized individuals. [Insert Practice Name] has established management controls for granting, changing, and terminating access to the computer system. These controls are essential to the security of [Insert Practice Name's] information system.

Security Procedures:

[Insert Practice Name] requires all of its employees to have effective and secure user IDs and passwords for access to [Insert Practice Name's] computer system. The Security Official or System Administrator will provide oversight of the process for administering and maintaining user IDs and passwords for [Insert Practice Name] as follows:

All employee passwords, even temporary passwords established for new and temporary employees, should meet the following characteristics:

Be easy for the employee to remember, but difficult for an unauthorized user to guess.

Be at least six characters in length.

Consist of a mix of alpha and at least one numeric or special character.

Be easy to type quickly.

Not be portions of associated account names (e.g., user ID, log-in name).

Not be portions of the employee‘s name (e.g., first name or last name in any form).

Not be the employee‘s spouse, children, or pets name in any form.

Not be information easily obtained about the employee (i.e., license plate numbers, telephone numbers, social security numbers, the brand of his/her automobile, the name of the street he/she lives on, date of birth, email name, etc.).

Not be character strings (e.g., abc or 123)

Assign each employee, including new and temporary employees, a unique user identification (user ID).

Assign each employee, including new and temporary employees, a unique temporary password

Furthermore, employees are required to select a new password immediately after their initial logon to the computer system using the temporary user ID and password.

Coordinate changing passwords at least every 30-90 days. Previously used passwords will not be re-used within x time period (e.g. every 2 yrs. or 4 password changes).

Disable user IDs and password accounts not used for 30 days and review such accounts for possible deletion. Review and delete accounts that have been disabled for 60 days. Review and delete password accounts for [Insert Practice Name] contractors on the expiration date of their contract.

Passwords will not be embedded in automated programs, utilities, or applications, such as: autoexec.bat files, batch job files, terminal hot keys.

Instruct employees to keep passwords confidential. Employees will be instructed to not share his/her password with anyone, including other employees, temporary employees, and contractors.

Remove vendor or service passwords from computer systems and assign new passwords to all computer systems immediately upon installation at [Insert Practice Name].

Passwords will not be visible on a data entry screen or display or documented in writing in any form (e.g., on a post-it note, on a message pad, on a calendar, on mobile device (e.g., smartphone, tablet), etc.).

Change passwords and disable user accounts promptly upon employee termination, including temporary employees, regardless of whether the termination was mandatory or voluntary. Users should immediately change their password if they suspect it has been compromised.

Limit employee log-on attempts to five (5) to prevent unauthorized access to the computer system by programming computer system account to ”lock up” or not provide further access by employee until discussion with System Administrator or Security Official.

Exhibit 6: Sample Anti-Virus Policies and Procedures

Sample Anti-Virus Policies and Procedures

_____
Insert Practice Name

Anti-Virus Policy:

[Insert Practice Name] is committed to taking the necessary steps to prevent computer viruses from infecting the practice's computer system. Practice employees must adhere to the policies and procedures listed below:

Employee should not open email attachments if he/she is not expecting an attachment from someone he/she knows or trusts.

Employees are strictly prohibited from using illegal or "pirated" software on the practice's computers.

Employees must scan files attached to email messages, files downloaded from the Internet, and files on CD-ROMs or thumb drives brought from home with anti-virus software prior to opening them in practice's computer system.

Employees are prohibited from installing and playing computer games on the practice's computer system.

Employees are prohibited from utilizing CDS, thumb drives, etc. on the practice's computer system if they suspect its files are infected with a virus.

Anti-Virus Procedures:

Employees must scan files attached to email messages, files downloaded from the Internet, and files on CD-ROMs or thumb drives brought from home using the practice's virus scanning software prior to being opened on the computer. The virus scanning software may automatically scan for viruses when files are

being downloaded onto the practice‘s computer system. If they are not, the employee must manually start the program.

The System Administrator or Security Official must conduct a virus scan of the practice‘s computer network server and workstations at least once a week. Employees should be instructed to log off, but not shut down their workstations once a week so the anti-virus software program can run in the evening.

When the practice purchases new computer software, the System Administrator or Security Official must make sure it is shrink-wrapped or downloaded from a reputable vendor and must check the software prior to installation on the computer system.

The System Administrator or Security Official must make sure that devices or other media of storage used to store computer software programs are ”write-protected” or protected against information from being saved on applicable storage media. This prevents viruses from being introduced into important storage devices which contain important information and thus corrupting the information.

If the practice obtains new computer equipment, but the ”new” computer is in reality a recycled one that someone else used before, the System Administrator, Security Official,
or information technology consultant installing the computer should conduct a ”low-level format” of the hard drive. This will destroy any viruses that may be on the hard drive as well as get rid of illegal copies of software.

If the practice obtains a recycled computer that comes pre-loaded with software or if the hard drive is pre-formatted, the System Administrator, Security Official, or information technology consultant should scan the hard drive for viruses before the practice starts using the computer.

All software should be acquired from reputable dealers.

Exhibit 7: Security Incident Report

Security Incident Report

_____

Insert Practice Name

Security Incident Report Number	
Report Date and Time	
Incident Type	Incident Description
Cause Suspected	Incident Location/Path
Anti-Virus Software Log Text (Print and Attach or Write Here)	
Computer User Name	
Workstation I.D.	
Additional Infected Systems Users	

Exhibit 8: Sample Backup Policy and Procedures

Sample Backup Policy and Procedures

_____
Insert Practice Name

Policy:

It is the policy of [Insert Practice Name] to implement backup procedures in order to protect the confidentiality, integrity, and availability of the electronic protected health information (EPHI) of our patients.

Procedures:

The System Administrator or Security Official is responsible for:

- Determining what information needs to be backed up.
- Determining type of backup data media, (e.g., CD, tape, etc).
- Maintaining the backup of the practice's server, systems, applications, and network.
- Testing the restoration process of all backed up data.
- Implementing full daily backups at the end of business day. Weekly backups will be retained for at least two months.
- Storing and retrieving backups off site.
- Implementing weekly backups of the operating system and network or as changes are made.
- Regularly testing the backup process assuring its ability to restore any lost data
- Either maintaining the backup procedures him/herself or delegating the responsibilities to another individual.

Practice employees and workforce members are responsible for:

- Saving their data incrementally (how often?) in order to avoid losing most recent inputs.
- Notifying the System Administrator, Security Official, or the backup designee immediately if his/her attempt to save EPHI fails.
- Notifying the System Administrator, Security Official, or the backup designee immediately if EPHI is compromised in any way.
- Backed up storage media must be labeled.
    1."Confidential"
    2. [Insert Practice Name]
    3. Date of backup
    4. Application or System backed up
    5. Version number

All media belonging to [Insert Practice Name] is assumed to contain sensitive information and should be treated as such.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Exhibit 9: Sample Security Incident Policy and Procedures

Sample Security Incident Policy and Procedures

_____

Insert Practice Name

Policy:

It is [Insert Practice Name's] policy to record and address attempts to incidentally or intentionally access Practice Name's physical space and/or the computer system and its components unless such access is authorized by the System Administrator or Security Official.

Procedures:

The practice will designate an individual who will be responsible for implementing and adhering to the practice's security incident policies and procedures.

The practice will determine through a variety of security mechanisms, such as User IDs, password protection, anti-virus software, and audit trails when security incidents have occurred.

The practice must periodically monitor user activity, including password activity, virus scans, and audit trails to determine if any security incidents have occurred.

Following the identification of a security incident, the practice's first priority must be to communicate the details of the incident to the relevant technical staff, such as the practice's technical staff or information technology consultant to expeditiously log and begin resolving the issue.

Once alerted to the incident, the appropriate staff will access the appropriate part of the computer system as quickly as possible. If more than one incident occurs simultaneously, the most critical issue will be addressed first.

The incident(s) will be immediately logged on a security incident log. The practice will take necessary and reasonable steps to respond to and address all identified and confirmed security incidents. All responses will be logged into a security incident log. The log will be kept for 6 years.

If the incident cannot be resolved and could potentially cause disruptions among other practice employees such that it will inhibit them from performing their assigned job responsibilities, the System Administrator or Security Official will notify the rest of the staff of the situation via email, telephone, verbally, or in writing. The practice

should select the communication media that works best under the circumstances. Affected staff will be notified of the estimated time necessary to address the security incident.

Once the issue has been resolved, the System Administrator or Security Official will notify practice staff of the resolution via email, telephone, verbally, or in writing. If there are new procedures which must take place as a result of the reported incident, these must be distributed to practice employees as well. The practice should select the communication media that works best under the circumstances.

The practice may wish to consider utilizing computer system alarms, if available, to identify critical computer system errors.

In the event that a security incident occurs, the Privacy Official should be notified and an investigation as to whether any EPHI has been compromised should take place. If a breach has occurred, appropriate notification must be made.

Exhibit 10: Sample Security Incident Log

Sample Security Incident Log

_____

Insert Practice Name

Incident	Time and Date Incident Reported	Time and Date Incident Occurred	Incident Reported By	Incident Handled By	Practice Individuals Notified	Responses
Virus discovered on Amy's computer	4:00 p.m. on 4/4/2013	4:00 p.m. on 4/4/2013	Amy	Security Official and Network Systems Ltd.	All	• Staff notified 4/4/2013 of virus on network Determine whether EPHI has been compromised • All staff instructed to leave computers on tonight for virus scan to run
Laptop computer missing	9:00 a.m. on 5/5/2013	Unknown	Ben	Security Official and Practice Administrator	Physician Owner	• Last laptop user questioned 5/5/2013 • Potential theft reported to building management Determine whether PHI has been compromised • Insurance carrier contacted re: replacement

Exhibit 11: Facility Maintenance Log

Facility Maintenance Log

____

Insert Practice Name

Date	Maintenance Issue	Who Repaired	Date of Repair

Exhibit 12: Sample Contingency Policy and Procedure

Sample Contingency Policy and Procedure

_____
Insert Practice Name

Policy:

It is the policy of [Insert Practice Name] to establish Contingency Plans in order to protect the confidentiality, integrity, and availability of our electronic protected health information from vulnerability in the event of an emergency. It is the purpose of [Insert Practice Name] to enable sustained operation of the information systems in the event of an extraordinary event that causes these systems to fail minimum production requirements. [Insert Practice Name] will assess the needs and requirements so that [Insert Practice Name] may be prepared to respond to the event in order to regain efficient operation of the systems that are damaged.

Procedure:

1. Every member of [Insert Practice Name's] workforce is responsible for the integrity of [Insert Practice Name's] electronic protected health information.

2. The Security Official (or other designated person) will respond to the Facility Security Analysis in order to determine if there are any vulnerabilities to the electronic protected health information of [Insert Practice Name].

3. The Security Official (or other designated person) will respond to the Contingency Plan steps for [Insert Practice Name].

4. [Insert Practice Name] will establish procedures in order to reduce the risk of vulnerability determined by the Facility Security Analysis.

5. The Contingency Plan of [Insert Practice Name] is an ongoing responsibility and will be reviewed by the Security Official of [Insert Practice Name] as necessary to include quarterly and annual reviews.

6. The Security Official (or other designated person) will train the workforce of [Insert Practice Name] on the procedures of the Contingency Plan.

7. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Exhibit 13: Contingency Plan Steps

Contingency Plan Steps

_____

Insert Practice Name

Practices need to analyze the criticality of their data:

1. Identify the key applications that support your electronic protected health information.
   Examples: practice management software, financial software, electronic medical records software, server.
2. Prioritize your identified applications.
3. Determine the estimated recovery time in the event of lost or damaged data.

Data backup plan:

1. Establish scheduled backups for identified key applications.
2. Identify who will be authorized to access the backed up data.
3. Identify off-site storage locations of your backed up data as well as hard copy documentation.
4. Document the location of the backup site and confirm that all parties understand the policy.

Disaster recovery plan:

1. Determine who will activate the Plan and how the Plan's activation will be communicated to the rest of the practice.
2. Determine if you will have hardware off-site or if you will be ordering or acquiring equipment after the fact.
3. Create specific tasks and responsibilities for those people designated within your practice responsible for data recovery.
4. Determine procedures for assessing damage as a result of a disaster.
5. Create a checklist to guide employees in the restoration process.
6. Create a complete list of all employee contact information.
7. Create a vendor contact list.
8. Organize vital records for the practice, such as server and workstation warranties.

Identify a range of events that may cause the total or partial relocation or suspension of practice operations:

1. Identify the facility (if relocation is an option) you will use during your emergency mode operations.
2. Determine your means of acquiring additional employee resources should your current employees be unable to quickly return to the practice.
3. Create a checklist to aid in the transition and restoration of your normal business operations.
4. Determine your communication plan for employees, business partners, and patients, including the resumption of post-disaster operations.

Testing and Revision:

1. Train all personnel on the policies and procedures regarding your contingency plans.
2. Determine if there are any weaknesses in your disaster and emergency operations plans.
3. Address any weaknesses discovered.
4. Update your disaster and emergency plans as necessary.
5. Schedule periodic testing of your disaster and emergency mode plans.

Steps to Activate Contingency Plan

Response Phase

Establish an immediate and controlled presence at the incident site.

Conduct a preliminary assessment of incident impact, extent of damage, and disruption to the information system and/or business operations.

Find and disseminate information on if or when access to the information system and/or facility will be allowed.

Provide senior management with the facts necessary to make informed decisions regarding subsequent resumption and recovery activity.

Resumption Phase

Establish and organize a management control center and headquarters for the resumption of operations.

Activate the support teams necessary to facilitate and support the resumption process.

Notify and appraise time-sensitive business operation resumption team leaders of the situation.

Alert employees, vendors, and other internal and external individuals and organizations.

Recovery Phase

Prepare and implement procedures necessary to facilitate and support the recovery of time-sensitive business operations.

Coordinate with the employees responsible for business operations and recovery.

Coordinate with employees, vendors, and other internal and external individuals and organizations.

Restorations Phase

Prepare and implement procedures necessary to facilitate the relocation and migration of business operations and technology to the new or repaired facility.

Manage the relocation/migration effort as well as perform employee, vendor, and customer notification before, during, and after relocation or migration.

Exhibit 14: Listing of Typical Business Associates

Listing of Typical Business Associates

_____
Insert 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

Lockbox Service

Collection agency

Accountant/consultant who needs access to PHI

Transcription service

Practice management software vendor that provides support or maintenance

Electronic medical records software vendor that provides support or maintenance

*Off-site record storage, including cloud storage providers

Hardware maintenance service

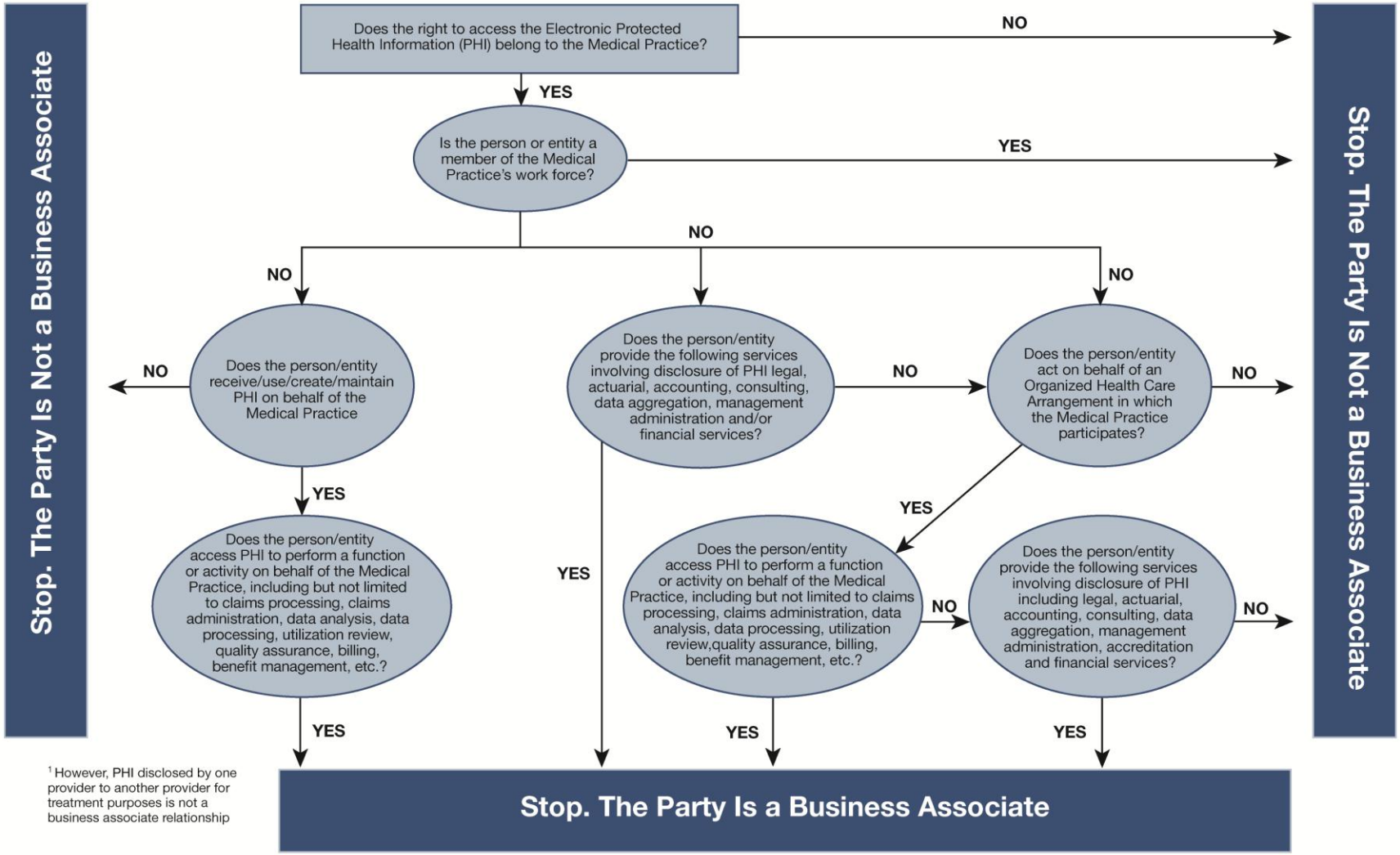
Other independent contractors who provide business/administrative services on-site and require access to PHI

THIS DOCUMENT IS A TEMPLATE. IT DOES NOT REFLECT THE REQUIREMENTS OF STATE LAW

Exhibit 15: A Medical Practice Guide for the Security Official to Identify Business Associates that Access PHI

(next page)

A MEDICAL PRACTICE GUIDE FOR THE SECURITY OFFICIAL TO IDENTIFY BUSINESS ASSOCIATIES THAT ACCESS PHI



[1] However, PHI disclosed by one provider to another provider for treatment purposes is not a business associate relationship

Exhibit 16: Sample Business Associate Agreement

LAWS: YOU SHOULD CONSULT WITH ADVISORS FAMILIAR WITH YOUR STATES PRIVACY LAWS AND LAWS REGARDING THIRD PARTY BENEFICIARIES PRIOR TO USING THIS DOCUMENT.

Sample Business Associate Agreement
(Security Rule Implementation)

_____
Insert Practice Name

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:
_____

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.

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 17: Sample Policy and Procedures on Workstation Use

Sample Policy and Procedures on Workstation Use

_____

Insert Practice Name

[Insert Practice Name] has adopted this policy on workstation use to comply with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 Security Standards. It is our duty to protect the confidentiality, integrity, and availability of our patient's electronic medical information as required by law. Physicians and staff of [Insert Practice Name] that use the practice's information system must be familiar with the contents of this policy and follow its guidance as appropriate when using computer equipment. As an employee of [Insert Practice Name], you are required to abide by the workstation use policy.

Operating Environment:

All computers owned by [Insert Practice Name] will be connected to surge protectors purchased by [Insert Practice Name].

Employees will monitor the computer system and report potential threats to the security of the data contained in the system to the Security Official of [Insert Practice Name]. All employees of [Insert Practice Name] will take appropriate measures to protect computers and data from disasters based on the policies and procedures of [Insert Practice Name].

The employees of [Insert Practice Name] should keep computer terminals, hard drives, keyboards, and screens clear of food and drink at all time.

The network and workstations have been configured according to standards provided by [Insert Practice Name]. The programs that have been installed are for the sole use of [Insert Practice Name]. All accessible data, personal or private, is for the sole use of [Insert Practice Name]. This includes data that employees may put on their local hard drives. The computer has been set up for your individual use solely for the business of [Insert Practice Name]. Employees of [Insert Practice Name] are not authorized to change any settings unless instructed by the Security Official. The Security Official monitors which software and hardware is at each workstation. Do not change anything without approval from the System Administrator.

Employees will not subject the practice's system to malicious programs (e.g., viruses, worms, etc.).

Passwords:

Employees are expected to maintain the confidentiality of their passwords. [Insert Practice Name] expects authorized users to be responsible for the security of their password.

Employees will log on to the system with their own password. Under no circumstances will an employee share their password with another employee or unauthorized person in order to allow them access to the system. [Insert Practice Name] monitors system access by authorized users.

Content:

Employees of [Insert Practice Name] will be held responsible for the content of any data entered into the system. This includes any information transmitted within the practice or outside the practice. An employee will not hide his/her identity as the author of any entry or represent that someone else entered the data or sent the message.

The Security Official of [Insert Practice Name] will issue access authorization to each employee. No employee may access any confidential patient or other information that they do not need to know. No employee may disclose confidential patient or other information, unless properly authorized.

Employees of [Insert Practice Name] may only use the computer system including email and fax capability for business purposes.

Printer:

When printing confidential patient information, employees are required to attend to the printer. Do not leave confidential information unattended on a company printer.

Log-Off:

(Practices will need to determine their log off requirements based upon their individual practice situations.)

When employees leave their computer terminal for any length of time, they are required to log-off the system. Emergent situations are the exception to this rule. The Security Officer of [Insert Practice Name] will determine emergent situations.

OR

When employees leave their computer terminal for any length of time, the system will automatically log off after ten minutes of idle screen time.

Screen savers will be programmed for each computer to activate after five minutes of idle screen time.

Backup Procedures:

Employees are required to adhere to the backup policies and procedures of [Insert Practice Name] with regard to all utilized applications.

Device and Media Controls:

Employees will use backup media (e.g., tapes, CDs, thumb drives, etc.) that are provided by [Insert Practice Name].

Employees will assume that all electronic media belonging to [Insert Practice Name] contains confidential information.

Destruction Procedures:

Employees are required to adhere to the destruction procedures of [Insert Practice Name] with regard to devices and media that contain EPHI.

Hard drives will be cleaned of all EPHI prior to its resell, donation, or disposal by use of appropriate ”cleaning” software.

Electronic media (e.g., tapes, CDs, thumb drives, etc.) will be destroyed via shredding or incineration prior to disposal.

Sanctions:

Any employee found to have violated this policy would be subject to disciplinary action, up to and including termination of employment.

The following are optional sections that you may wish to include in your Workstation Use Policy

Optional:

Portable Computers

The laptop computers are the sole property of [Insert Practice Name]. The laptops are for off-site work based upon prior approval from your supervisor.

The laptops must be checked out from the Security Official so that they can be kept track of for other employees to use.

The laptops are set up by the Security Official when they are purchased. Data needed should be saved on a CD or thumb drive, not to the laptop hard drive. If the data files you need are too large for CDs or thumb drives, the Security Official will load them on the laptop via the network.

When you return to the office, all data must be removed from the laptops immediately, particularly if the files are too large to put on a CD.

The laptop will then be checked back in by the Security Official.

When working off-site, you should find some way to keep the data separate from the laptop. In addition, the laptop should be turned off when you are not actively working on it in order to avoid disclosure of confidential or sensitive data. Data security is a must when you are away from the practice setting.

Employees are accountable for the security of the laptop while in their possession. If the equipment is stolen, employees are to report the theft immediately.

Optional:

Electronic Mail

The Email system should only be used for work related purposes. [Insert Practice Name] reserves the right to monitor Email and Internet usage.

Due to system restrictions and space limitations, no pictures, graphics, movies, or any other Email file attachments should be in the system without a viable business reason.

Forgery (or attempted forgery) of electronic mail messages is prohibited.

Attempts to read, delete, copy, or modify the electronic mail of other users are prohibited.

Attempts at sending harassing, obscene, or threatening email to another user are prohibited.

Attempts at sending junk mail, ”for-profit,” or chain email is prohibited.

Optional:

Internet Access

[Insert Practice Name] authorizes the availability of the Internet/World Wide Web to provide access to Internet resources that will enhance and support business activities. It is expected that employees will use the Internet to improve their job knowledge and to access information on topics which have relevance to [Insert Practice Name].

Employees who do not require access to the Internet as part of their official duties will not be given access.

Employees should be aware that when access is accomplished using Internet addresses and domain names registered to [Insert Practice Name], they may be perceived by others to represent [Insert Practice Name]. Users are advised not to use the Internet for any purpose that would reflect negatively on [Insert Practice Name] or its employees.

The computer system of [Insert Practice Name] is not for personal use; however, when certain criteria is met, users are permitted to engage in the following activities:

- During working hours, access job-related information, as needed, to meet the requirements of their jobs.
- During working hours, participate in Email discussion groups (list servers), provided these sessions have a direct relationship to the user‘s job with [Insert Practice Name]).

The following uses of the Internet, either during working hours or personal time, using [Insert Practice Name‘s] equipment or facilities, are not allowed:

- Access, retrieve, or print text and graphics information that exceeds the bounds of generally accepted standards of good taste and ethics.

- Engage in any unlawful activities or any other activities that would in any way bring discredit on [Insert Practice Name].
- Engage in personal commercial activities on the Internet, including offering services or merchandise for sale or ordering services or merchandise from on-line vendors.
- Engage in any activity that would compromise the security of [Insert Practice Name].
- Obtaining personal files via the Internet on individual PC hard drives or on local area network (LAN) file servers.
- Game playing of any kind.
- Propagating any computer virus.
- Maintaining a secret pass code.

Employees will follow existing security policies and procedures in their use of Internet services and will refrain from any practices that might jeopardize the computer systems and data files, including but not limited to virus attacks, when downloading files from the Internet.

Employees using equipment owned by [Insert Practice Name] to access the Internet are subject to having activities monitored by the Security Official. Use of this system constitutes consent to security monitoring and employees should remember that most sessions are not private.

Confidential information is not to be transmitted over the Internet without encryption.

Optional:

Smartphones and Tablets

Smartphones and tablets are not considered a secure computing device. It is recommended that only non-confidential information be stored on the device and the password protection feature enabled.

The Security Official must approve installation of a smartphone device and associated software. A valid business reason must be demonstrated beyond the use of the personal information management (PIM) features (e.g., calendar, phone list, to-do list).

All smartphones or tablets connected to the [Insert Practice Name] network, whether supplied by the employee or [Insert Practice Name], shall comply in total with the standards for hardware and software.

[Insert Practice Name] has the right to require the removal of specific software or files from smartphones or tablets connecting to the network, whether employee- or [Insert Practice ENxhaibmit eon]-CD-ROM owned.

[Insert Practice Name]-owned smartphones or tablets are assigned to a specific position. When a position for which a smartphone or tablet was approved is vacated, [Insert Practice Name]-owned smartphones, tablets, software, and accessories will be returned to that position‘s supervisor.

Employee-owned: Upon leaving the position for which a smartphone or tablet was approved, all [Insert Practice Name]-owned software or information will be removed and [Insert Practice Name]-owned software and accessories will be returned to Security Official.

[Insert Practice Name] will provide support for installation of [Insert Practice Name] standard software in connection with smartphones and tablets. Support for smartphone or tablets hardware is via the hardware vendor or wireless carrier. [Insert Practice Name] will perform problem determination activities to establish whether a problem is hardware or software related.

All smartphones or tablets connected to the [Insert Practice Name] network environment, whether employee- or [Insert Practice Name]-owned, shall have password protection enabled.

All smartphones and tablets may be inspected on a yearly basis for existence of unauthorized software or organization data. (Unauthorized Software: For the purposes of this policy, unauthorized software shall include software not licensed for use by [Insert Practice Name], unauthorized duplicate of licensed software, software where proof of ownership cannot be established, or software specifically disallowed by [Insert Practice Name].

Optional:

Remote Access

This policy applies to [Insert Practice Name's] employees, contractors, vendors, and agents with a [Insert Practice Name]-owned or personally-owned computer or workstation used to connect to the [Insert Practice Name's] network. This policy applies to remote access connections used to do work on behalf of [Insert Practice Name], including reading or sending email and viewing intranet web resources. Remote access means any access to [Insert Practice Name's] network through a non-[Insert Practice Name] controlled network device or medium.

Employees, contractors, vendors, and agents with remote access privileges to [Insert Practice Name's] network are required to ensure that their remote access connection is given the same consideration as the user's on-site connection to [Insert Practice Name].

Please review the encryption policy for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of [Insert Practice Name's] network.

Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication.

At no time should any [Insert Practice Name] employee provide his/her login or email password to anyone, not even family members.

Employees with remote access privileges must ensure that their [Insert Practice Name] owned or personal computer or workstation, which is remotely connected to the practice's network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

Employees with remote access privileges to [Insert Practice Name's] network must not use personal email accounts (i.e., Gmail, Yahoo!,), or other external resources to conduct [Insert Practice Name] business, thereby ensuring that official business is never confused with personal business.

Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

Frame Relay must meet minimum authentication requirements of DLCI standards.

All hosts that are connected to [Insert Practice Name] internal networks via remote access technologies must use the most up-to-date anti-virus software (place URL) to corporate software site here), which includes personal computers. Third party connections must comply with requirements as stated in the Third Party Agreement.

Personal equipment that is used to connect to [Insert Practice Name's] networks must meet the requirements of [Insert Practice Name's] owned equipment for remote access.

Exhibit 18: Security Policy Training Checklist

Security Policy Training Checklist

_____
Insert 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 Security Rule

_____ Introduction of the Security Official and Overview of Security Official

Responsibilities:

_____ Explanation of Workforce Confidentiality Agreements

_____ Overview of Practice's Security Policies and Procedures

_____ Workstation Use

_____ Workstation Security

_____ Virus Protection

_____ Login Monitoring

_____ Password Management

_____ Data Backup and Storage

_____ Contingency Plans

_____ Explanation of Who Can Access EPHI

_____ Discussion of Job Responsibilities as it Relates to EPHI

_____ Explanation of Minimum Necessary Standard

_____ Explanation of Sanctions

Exhibit 19: Training Documentation Form

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

Workforce Confidentiality Agreement

_____
Practice Name

I understand that_____has a legal and ethical responsibility to 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 financial data and operational information pertaining to the practice that's obligated to maintain as confidential.

As a condition of my employment/assignment/affiliation with_____, 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.

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 purging 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).

Upon termination of my employment/assignment/affiliation with _____, I will immediately return all property (e.g. keys, documents, ID badges, etc.) to_____.
I agree that my obligations under this agreement regarding Patient Information will continue after the termination of my employment/assignment/affiliation with_____.

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 suspension, restriction or loss of privileges, in accordance with_____'s policies, as 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.

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: Sample Workforce Termination Procedures

Sample Workforce Termination Procedures

_____

Insert Practice Name

The System Administrator or Security Official will be responsible for ensuring the following procedures take place immediately upon an individual's termination from the practice. Doing so will revoke an individual's access to the physical office as well as access to the computer system.

Prior to the individual's departure, the System Administrator or Security Official will:

- Contact a locksmith to change the practice locks, if necessary.
- Secure a full computer backup tape.
- Instruct individual whether or not to clean out his/her computer hard drive, if appropriate.
- Retrieve the following from the individual prior to departure:
    - Backup tapes and other removable storage devices such as thumb drives;
    - Keys
        - Office
        - Safe
        - Desk
        - Filing cabinets
        - Mailbox
        - Keycards (building; parking deck)
    - Computer System Passwords
        - Network passwords
        - Email passwords
        - Additional passwords
- Retrieve and secure practice property, including laptops, smartphones/cell phones, and tablets.

- Have office locks changed, if needed. If the practice utilizes a door lock with a key pad, the key pad numbers must be changed.

- Circulate new keypad code numbers and office keys to pertinent practice employees, if necessary.

- Change or delete (as applicable) passwords to the computer workstation, network, and all email/internet accounts.

Exhibit 22: Workforce Termination Checklist

Workforce Termination Checklist

_____

Insert Practice Name

Task	**Task Name of Individual Completing Task**	**Date Completing Task**
1. Contact a locksmith to change the practice locks, if necessary.		
2. Secure a full computer backup tape.		
3. Instruct individual whether or not to clean out his/her computer hard drive, if appropriate.		

4. Retrieve the following from the employee prior to departure: Backup tapes (including removable storage devices such as thumb drives)
• Keys
  • Office
  • Safe
  • Desk
  • Filing cabinets
  • Mailbox
  • Keycards (building; parking deck)
• Computer system passwords
  • Network passwords
  • Email passwords
  • Additional passwords		

Task	**Name of Individual Completing**	**Date Task Completed**
5. Retrieve and secure practice property: Laptops Tablets Cell phones/Smartphones Files Books Records Pagers Manuals Vehicles Patient lists		

Rolodexes		
6. Have office locks changed, if needed. If the practice utilizes a door lock with keypad, the keypad code numbers must be changed.		

Task	**Name of Individual Completing**	**Date Task Completed**
7. Circulate new keypad code numbers and keys to office.		
8. Change applicable passwords to the computer workstation, network, and all email/internet accounts to prevent access through outside means.		
9. Prepare pre-termination and post-termination audit trails documenting employers Workstation/password activity pre and post termination.		
10. Conduct limited audit of patient information and financial information. (Contingent upon employee‘s degree of access).		

Exhibit 23: Sample Sanction Policy

Sample Sanction Policy

_____

Insert Practice Name

[Effective Date]

[Insert Practice Name] has adopted this Sanction Policy as of the above Effective Date to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the regulations requirement for such a policy, as well as to fulfill our duty to protect the confidentiality and integrity of confidential electronic medical information as required by law.

[Insert Practice Name] has adopted a Security Policy requiring [Insert Practice Name] and its physicians, staff, and agents to protect the integrity and confidentiality of electronic medical and other sensitive information pertaining to our patients. In addition, [Insert Practice Name] has adopted policies and standards to carry out the objectives of the Security Policy. Each of these policies and standards notes that all providers, staff, and agents of [Insert Practice Name] must adhere to these policies and standards, that [Insert Practice Name] will not tolerate violations of these policies and standards, and that such violations constitute grounds for disciplinary action up to and including termination, professional discipline, and criminal prosecution.

Any provider, staff, or agent of [Insert Practice Name] who believes another provider, staff, or agent of [Insert Practice Name] has breached the facility's security policy or the policies and standards promulgated to carry out the objectives of the Security Policy or otherwise breached the integrity or confidentiality of patient or other sensitive information should immediately report such breach to his or her supervisor or to the Security Official for [Insert Practice Name].

The Security Official for [Insert Practice Name] will conduct a thorough and confidential investigation into the allegations. The Security Official will inform the complainant of the results of the investigation and any corrective action taken. [Insert Practice Name] will not retaliate against or permit reprisals against a complainant. Allegations not made in good faith, however, may result in discharge or other discipline.

[Insert Practice Name] has a progressive discipline policy under which sanctions become more severe for repeated infractions. This policy, however, does not mandate the use of a lesser sanction before [Insert Practice Name] terminates an employee. In the discretion of management, [Insert Practice Name] may terminate an employee for the first breach of the facility's security policy or individual policies and standards if the seriousness of the offense warrants such action. An employee could expect to lose his or her job for a willful or grossly negligent breach of confidentiality, willful or grossly negligent destruction of computer equipment or data, or knowing or grossly negligent violation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), its implementing regulations, or any other federal or state law protecting the integrity and confidentiality of patient information and may lose his or her job for a negligent breach of [Insert Practice Name's] standards for protecting the integrity and confidentiality of patient information. For less serious breaches, management may impose a lesser sanction, such as a verbal or written warning, verbal or written reprimand, loss of access, suspension without pay, demotion, or

other sanction. In addition, [Insert Practice Name] will seek to include such violations by contractors as a ground for termination of the contract and/or imposition of contract penalties.

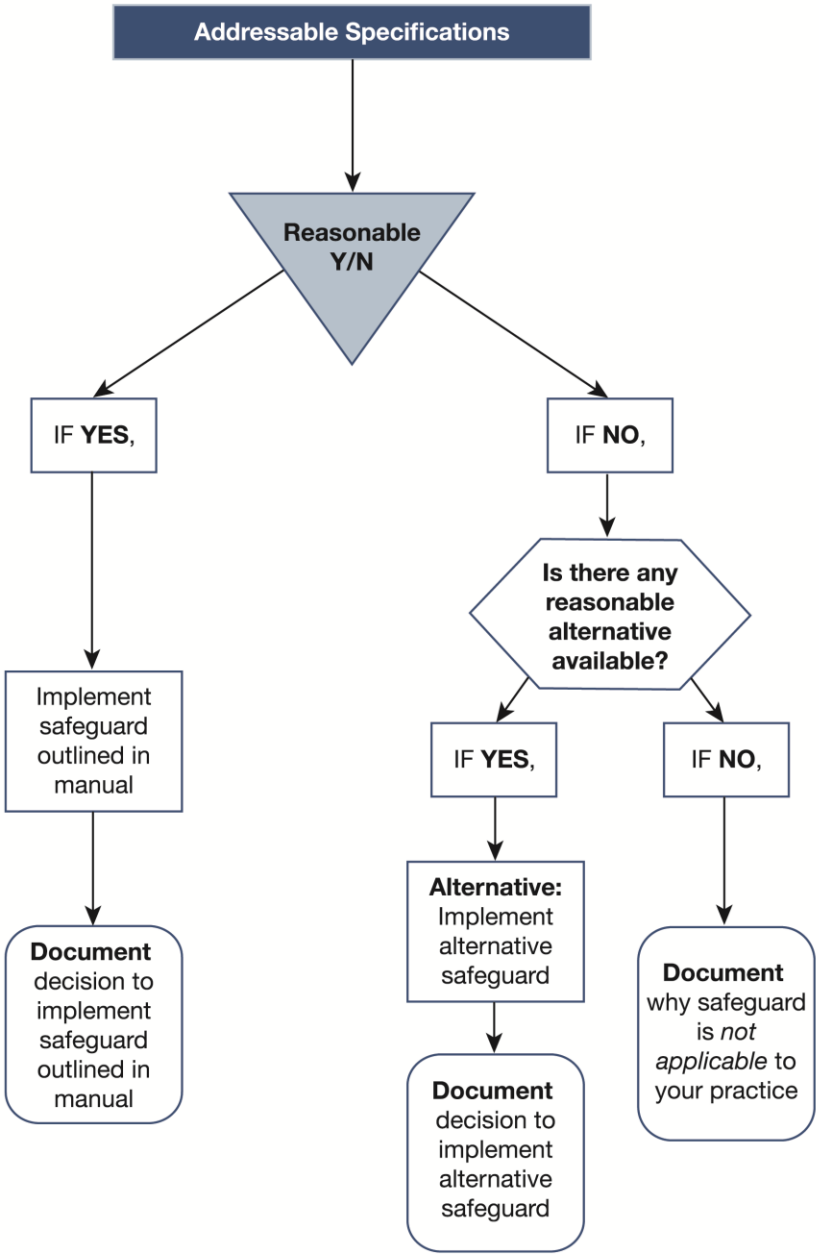
Violation of the facility's security policy or individual policies and standards may constitute a criminal or civil offense under HIPAA, other federal laws, such as the Federal Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030, or state laws. Any employee or contractor who violates such laws may expect that [Insert Practice Name] will provide information concerning the violation to appropriate law enforcement personnel or authorities and will cooperate with any subsequent investigation or prosecution.

Further, violations of the facility's security policy or individual policies and standards may constitute violations of professional ethics and be grounds for professional discipline. Any individual subject to professional ethics guidelines and/or professional discipline should expect [Insert Practice Name] to report such violations to appropriate licensure/accreditation agencies and to cooperate with any professional investigation or disciplinary proceedings.

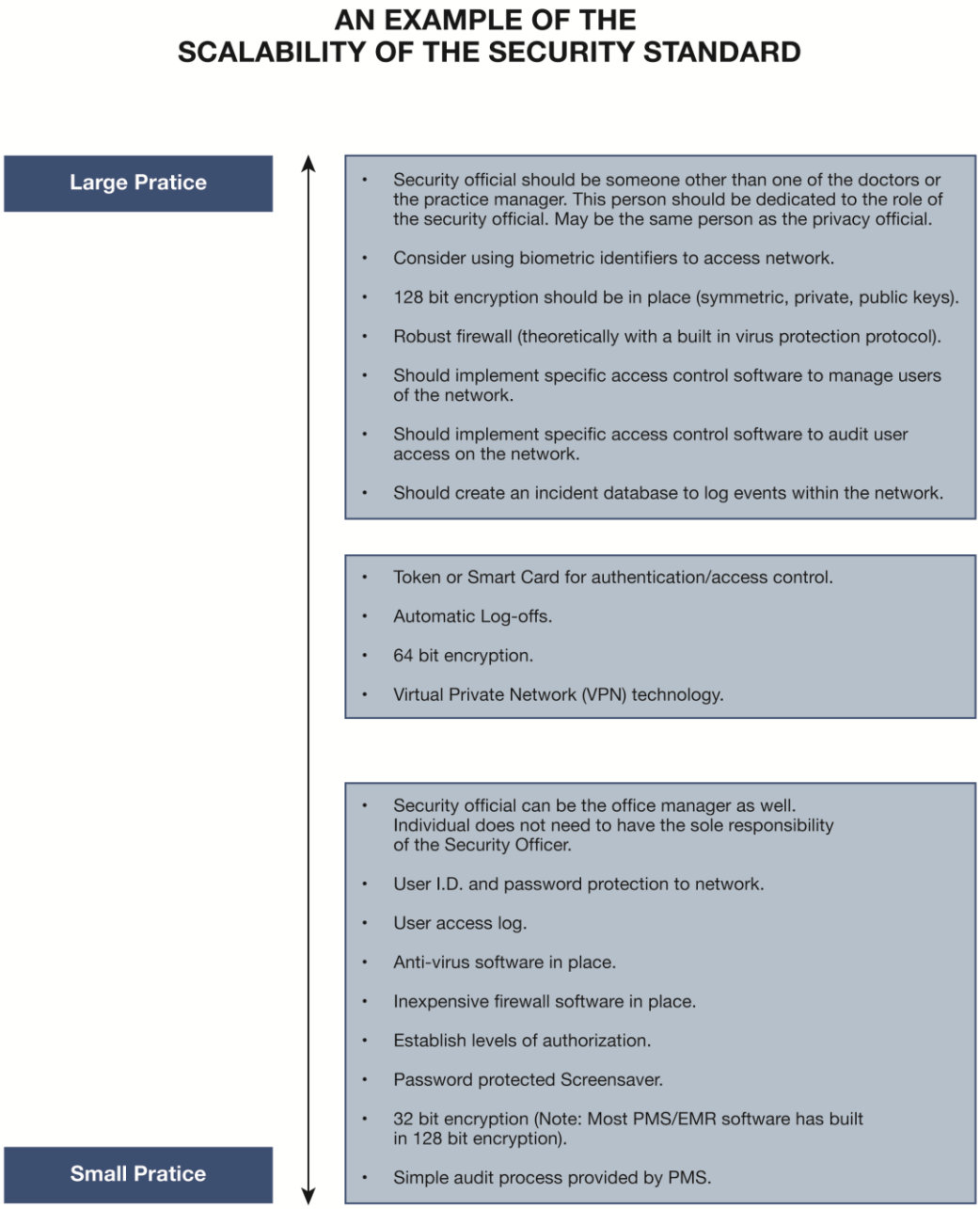
This Sanction Policy is intended as a guide for the efficient and professional performance of employee's duties to protect the integrity and confidentiality of medical and other sensitive information. Nothing herein shall be construed to create a contract between the employer and the employee. Additionally, nothing in this Sanction Policy is to be construed by any employee as containing binding terms and conditions of employment. Nothing in this Sanction Policy should be construed as conferring any employment rights on employees. Management retains the right to change the contents of this Sanction Policy as it deems necessary with or without notice, provided however, that employees will be notified of any such changes.

All officers, employees, and agents of [Insert Practice Name] are expected to comply and cooperate with the facility's administration of this policy.

Appendix 1: Addressable Specifications



Appendix 2: Security Standard Scalability Example



Appendix 3: HIPAA Resources

HIPAA Resources

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