APMA

HIPAA Security Manual

Published by the
American Podiatric
Medical Association, Inc.

AMERICAN PODIATRIC MEDICAL ASSOCIATION, INC.

July 2004

Dear Colleague:

The American Podiatric Medical Association (APMA) is pleased to provide the APMA Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Manual as a free, on-line member benefit. It can be downloaded in Word and customized for individual use by members. The new APMA HIPAA Security Manual is the third manual produced for members in the last three years and again demonstrates the value of APMA membership.

The Manual addresses the rules and regulations regarding the security of patients' electronic Protected Health Information (ePHI) and will assist podiatric physicians in complying with the Security Rules issued by the Department of Health and Human Services. **The deadline for compliance with the Security Rule is April 21, 2005.**

The APMA HIPAA Security Manual is intended to be an additional tool and template for podiatric physicians and should be used in conjunction with the APMA HIPAA Privacy Manual, published by the APMA in 2002. As with the Privacy Rule, the Security Rule is not optional for covered health care providers.

J. Kevin West of the law firm of Hall, Farley, Oberrecht & Blanton, P.A. authored the Manual, which is intended for use by APMA member podiatrists throughout the United States.

Be advised that this Manual does not constitute legal advice nor does it establish a standard of care since individual circumstances vary. Users of this Manual are encouraged to discuss their specific security compliance matters with a competent health care attorney or consultant.

The Manual is copyrighted by APMA and should not be distributed to individuals who are not members of the APMA. To those who are members, enjoy this latest member benefit!

Lloyd S. Smith, DPM
President

Ross E. Taubman, DPM
Chair, Health Policy Committee

Michael J. King, DPM
Chair, Health Systems Committee

9312 Old Georgetown Road Bethesda, Maryland 20814-1621
(301) 571-9200 Fax (301) 530-2752 http://www.apma.org

APMA HIPAA

Security Manual

Authored by J. Kevin West

APMA HIPAA
Security Manual

Authored by J. Kevin West
HALL, FARLEY, OBERRECHT & BLANTON, P.A.

DISCLAIMER

This Manual is designed to set forth general policies and procedures that will satisfy the requirements of the HIPAA Security Rule in the context of small to medium size podiatry practices. Every effort has been made to ensure accuracy and thoroughness. However, this Manual does not constitute legal advice. It is strongly recommended that all podiatrists consult with competent health care counsel as they seek to finalize and implement the policies and procedures contained herein. In particular, counsel should be consulted regarding potential conflicts with state laws. The provisions in this Manual may need to be modified to fit certain practitioners' specific individual circumstances.

TABLE OF CONTENTS

INTRODUCTION

About this Manual

Under the authority of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Department of Health and Human Services (HHS) has promulgated rules and regulations regarding the security of patients' electronic Protected Health Information (ePHI). These rules will be referred to in this Manual as the HIPAA Security Rule (Security Rule). The deadline for compliance with the Security Rule is April 21, 2005.

The Security Rule encompasses protections for electronic protected health information that are in addition to the protections contained in the HIPAA Privacy Rule, which took effect in April 2003. As with the Privacy Rule, compliance with the Security Rule is not optional for health care providers. The Security Rule is a requirement of federal law and will require all health care providers to implement written policies and procedures, as well as certain changes in office practices.

This Manual is intended to be an additional tool and template for podiatric physicians to be used in conjunction with the APMA HIPAA Privacy Manual, published by the APMA in 2002. Not every policy, however, will necessarily apply to your practice in the exact form contained herein. Accordingly, you should consult with legal counsel and technical consultants in implementing these policies.

About the Author

J. Kevin West is a partner with the firm of Hall, Farley, Oberrecht & Blanton, P.A. in Boise, Idaho. For over eighteen years, he has represented health care providers, including podiatric physicians, in a wide variety of legal matters such as medical malpractice, licensure, Medicare compliance and audit defense business transactions and, most recently, HIPAA compliance. Mr. West was the author of the APMA HIPAA Privacy Manual. For the past four years, he has served as national counsel for a major podiatric malpractice insurer in supervising Medicare and other regulatory claims brought against its insureds. Mr. West is a nationally recognized author and lecturer on health care law and risk management issues. He authored the nationally marketed publication, Medicare Compliance: A Training Program for Podiatrists and Their Staff. He has lectured throughout the United States on the subject of HIPAA compliance. Mr. West is a member of the Idaho HIPAA Coordinating Council, a task force assigned by the Idaho Medical Association to educate its 12,000 members regarding HIPAA issues. Mr. West acknowledges the able assistance of his associate, Jill M. Twedt, in preparing this Manual.

Who and What is Regulated by the Security Rule?

Those medical providers and practices who currently (or in the future) must comply with the HIPAA Privacy Rule must also comply with the Security Rule. The Security Rule applies to all Protected Health Information stored or maintained in electronic formats ("electronic Protected Health Information" or "ePHI"). The following are common examples of ePHI:

- Patient medical and billing records maintained on the Practice's computer system
- Patient information transmitted via the Internet
- Claims for payment transmitted electronically to payors
- Emails containing patient information or communications
- Patient information in laptops, PDAs and cell phones

Commonly Used Terms

The following abbreviations and shorthand expressions will be used for ease of reference in this Manual:

HHS	Health and Human Services
Practice	The podiatry practice or office which implements or uses this Manual.
Practice personnel	All personnel, including podiatric physicians, whether owners or otherwise, and their staff, in the podiatry practice.
Patient health information	"Protected Health Information," as defined by HIPAA (see Glossary of Terms).
Electronic PHI or ePHI	"Protected Health Information," in an electronic format.
Manual	This APMA HIPAA Security Manual
HIPAA	Health Insurance Portability and Accountability Act of 1996

POLICIES AND PROCEDURES

Section A: An Introduction to Basic Security Concepts and Compliance

Section B: Administrative Safeguards

Section C: Physical Safeguards

Section D: Technical Safeguards

Section A: An Introduction to Basic Security Concepts and Compliance

1. Purpose of the Security Rule

The four general goals of the Security Rule are to:

- Ensure the confidentiality, integrity and availability of all ePHI that a health care provider creates, receives, maintains or transmits;

- Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;

- Provide additional protection against uses or disclosures of ePHI that are not permitted or required by the Privacy Rule; and

- Ensure compliance by the health care provider's workforce.

The Privacy Rule and Security Rule are closely linked. Privacy is the "who, what and when" for privacy and confidentiality issues; Security is the "how." The purpose of the Security Rule is to ensure that providers have policies and procedures in place to protect the confidentiality, integrity and availability of ePHI. Confidentiality, integrity and availability are the three key elements of security.

2. Security Rule Concepts

The Security Rule was written to be flexible enough to be implemented by either large or small practices. Though the Rule involves many technical matters, no particular brand or technology is required. In most instances, practices should be able to continue the use of existing technology.

The Security Rule consists of eighteen standards, which are organized into the following three categories:

- **Administrative Safeguards** – Administrative safeguards are the policies and procedures the Practice should implement to protect ePHI.

- **Physical Safeguards** – Physical safeguards are the security measures that protect the Practice's physical facility and information systems. Physical safeguards require the restriction of access to ePHI through the use of such things as door locks or magnetic cards, and by providing backups for all ePHI, such as having a second computer hard drive to perform a daily backup of computer programs containing ePHI.

- **Technical Safeguards** – Technical safeguards are the security measures installed to protect information contained in the information systems. Examples of technical safeguards include individual passwords for each employee accessing ePHI, ensuring that the person accessing ePHI is authorized and is who he/she claims to be, and ensuring that information contained in ePHI is not improperly altered.

For each of the eighteen standards found in these three safeguard categories, there are accompanying "implementation specifications." The eighteen standards describe what must be done to achieve security compliance; the implementation specifications describe how compliance with a standard may be accomplished. Some of the implementation specifications are mandatory; others are optional. The mandatory specifications are referred to in the Security Rule as "required specifications;" the optional specifications are referred to as "addressable specifications." If the Practice chooses not to implement an addressable specification, it must document the reason for that choice and what, if anything, is being done in its place. Appendix J provides a checklist of the required and addressable specifications for each of the eighteen standards found in the three safeguard categories.

The goal of the Security Rule is to decrease and/or eliminate security incidents. A "security incident" is some breach of confidentiality, integrity or accessibility of the Practice's ePHI. A security incident may be the result of a "threat" (anything that could harm the Practice's information system, such as hackers, natural disasters or disgruntled Practice personnel), that takes advantage of a "vulnerability" (any weakness in the Practice's security measures or information systems).

3. How to Begin

Before performing surgery on a patient, health care providers routinely perform a "history and physical" in order to evaluate the patient's condition and plan a course of treatment. Compliance with the Security Rule involves a similar process. Using the materials in Section B.3, and Appendix A, you should do an inventory of your current electronic systems and equipment and evaluate the potential security risks inherent in those systems and equipment. The Security Rule refers to this process as a "Risk Analysis." It is strongly recommended that you have someone with technical expertise to consult with you in doing your Risk Analysis. Your current computer system vendor or practice management software vendor could be valuable places to obtain some of this technical assistance. The steps for conducting a Risk Analysis may be found in Section B.3.

Completion of the Risk Analysis will help you determine those additional steps that your Practice should take to be in compliance with the Security Rule. Note that the policies in Sections B, C and D of the Manual correspond with the "to do" list items in the Risk Analysis. These materials will assist in providing the written policies and procedures your Practice needs to achieve compliance.

Using This Manual

Sections B, C, and D set forth the policies and procedures which most health care practitioners will need to implement to comply with the HIPAA Security Rule. Following each policy/procedure is a "Practice Guidance" section which provides explanation as to how to implement the accompanying policy/procedure in your practice. The Practice Guidance materials are tutorials designed to teach and train Practice personnel in how to implement the provisions of this Manual.

Section B: Administrative Safeguards

1. Personnel Designations

Security Officer. The Practice will designate a person to act as its security officer. The security officer will have responsibility for the overall implementation and oversight of the Practice's compliance with the HIPAA Security Rule. The same person may be designated as both security officer and privacy officer. Specifically, the security officer will:

- Oversee the implementation of the policies and procedures contained in this Manual.
- Ensure that all Practice personnel are trained regarding the policies and procedures in this Manual as appropriate for their positions and job functions.
- Provide a copy of this Manual to all Practice personnel and ensure that such personnel follow the policies and procedures contained herein.
- Investigate and respond to security incidents and take appropriate action in response.
- Maintain all documentation required by this Manual and the HIPAA Security Rule.
- Review activity that takes place in all Practice information systems to detect possible Security Rule violations and security incidents.
- Respond appropriately to all security incidents and eliminate or mitigate any damaging effects.

Practice Guidance

The HIPAA Security Rule requires that your practice formally appoint someone to serve as security officer for the Practice. A resolution form (Practice Resolution for Appointment of Security Officer) for this purpose may be found in Appendix E to this Manual.

The security officer may be either an employee of the Practice or a third party that you retain for that purpose. Some practices may wish to use a technical consultant. If you use an outside party, however, they must still be able to satisfy the responsibilities listed in the seven bullet points contained in the policy above.

Your security officer and privacy officer may be the same person. In small practices, it may make sense for the office manager to fulfill both roles. If your office manager acts as your security officer, he/she should have someone to consult with regarding technical issues. As discussed in the other Practice guidance sections of this Manual, the Security Rule is highly technical and compliance decisions will often involve the need for hardware, software, server or network expertise.

2. Training of Practice Personnel

2.1 **Training – Generally.** The Practice will train all Practice personnel regarding the HIPAA Security Rule, as well as this Manual, as is reasonable and appropriate for personnel to carry out their respective job duties. Appendix I contains an acknowledgment of receipt and review of this Manual for all Practice personnel to sign.

2.2 **Time for Completion of Training.** Initial training of existing Practice personnel will be completed prior to April 21, 2005. Training of employees hired after April 21, 2005 will be completed within sixty (60) days of hiring. Ongoing training will be provided to Practice personnel as necessary to maintain competency regarding HIPAA policies and procedures, or as needed for changes in the HIPAA Security Rule or this Manual.

2.3 **Documentation of Training.** Training of Practice personnel will be recorded in the Security Training and Education Log (Appendix D), and this log will be maintained by the Practice for a minimum of six (6) years.

2.4 **Methods of Training.** The Practice owners and security officer will use their discretion as to the method, location and frequency of training. Such training may, however, include some or all of the following:

- In-service meetings among Practice personnel for updates in the Security Rule.
- Review of this Manual.
- Attendance at programs and seminars.
- Review of professional literature and publications.
- Use of Internet resources (Appendix H).
- Retained consultants and professional advisers.

Practice Guidance

Like the HIPAA Privacy Rule, the Security Rule also mandates training of Practice personnel. As the regulations state: "Security awareness training is a critical activity regardless of an organization's size."

With respect to general security awareness, training should include all Practice personnel. More in depth training may be necessary for certain personnel, particularly the security officer. Training will be based on the policies and procedures contained in this Manual. Each policy should be discussed with Practice personnel in order to create awareness of basic security concepts. More in depth training for the security officer would likely include such issues as virus protection, computer and network firewalls, monitoring login success/failure, password management, system break-ins and emergency planning.

HIPAA training for Practice personnel need not be burdensome or time-consuming. Devoting one lunch hour per calendar quarter would likely be adequate for most small practices. The Log found in Appendix D should be used to document all training and education of Practice personnel.

3. Security Management

3.1 **Security Assessment of the Practice.** Using the Risk Analysis Checklist in Appendix A, the Practice will conduct an accurate and thorough assessment of the current status of the Practice's security compliance. Using the checklist will help the Practice identify potential threats and vulnerabilities to the confidentiality, integrity and accessibility of ePHI held by the Practice. The Practice may need to enlist the assistance of a technical consultant.

3.2 **Implementation of Security Measures.** Based upon the information obtained in the security assessment, the Practice will implement through this Manual the necessary policies and procedures to address the risks and vulnerabilities of the Practice's ePHI.

3.3 **Enforcement of Security Policies.** All Practice personnel are expected to adhere to the policies and procedures set forth in this Manual. Practice personnel who violate the provisions of this Manual will be subject to discipline, which may include:

- A written warning in the employee's personnel file.
- Placement on probation.
- Mandatory additional training regarding the HIPAA Security Rule.
- Demotion or reassignment of job duties.
- Termination.

The security officer will maintain a record of all disciplinary action for a minimum of six (6) years.

3.4 **Reporting of Security Violations.** Practice personnel are required to report any violation of the provisions of this Manual, and any security incident, to the security officer. The Practice will not retaliate against any employee for reporting these matters. The security officer will track security incidents on the security incident tracking report (see Appendix F).

3.5 **Prevention of Further Violations.** To the extent that security incidents or deficiencies are reported or discovered, the Practice will take reasonable steps to ensure that similar violations do not occur in the future by taking appropriate corrective measures.

3.6 **Regular Review.** The security officer will regularly review records of all information system activities for possible security incidents and will implement procedures to correct possible and/or known security incidents. The Practice's information system should also be checked frequently and regularly to ensure that daily back-ups have been done and that intrusions into the system have not occurred.

Practice Guidance

The subject of "security management" in a medical practice includes the creation, administration and oversight of policies and procedures to present, detect and correct security violations that could compromise ePHI.

Accordingly, security management is an all-encompassing concept that includes these areas:

- Risk analysis
- Risk management
- Policies and procedures
- Enforcement of policies and procedures

Risk Analysis. A health care provider, such as a doctor, takes a patient history, performs a physical examination and lab tests to evaluate a patient's medical condition and assess health problems. A similar process should take place regarding your Practice's electronic security. A risk analysis is a "history and physical" of your practice from a security standpoint. The Risk Analysis Checklist found in Appendix A is a tool designed to help a small practice in evaluating its compliance with certain basic HIPAA security requirements.

Risk Analysis Steps. The following are suggested steps to complete the "risk analysis" required by HIPAA:

Step One: Complete the Risk Analysis Checklist found in Appendix A.

Step Two: Threat Identification – Identify all potential threats to ePHI. The following are examples of threats:

- Natural – flood, earthquake, etc.
- Human – hackers, viruses, disgruntled past or present employees
- Environmental – extended power outage, pollution, chemicals

Step Three: Vulnerability Identification – Identify weaknesses in the computer security systems that make ePHI vulnerable to the identified threats.

Examples of vulnerabilities:

- Software or hardware becoming obsolete
- Failure to update software
- Lack of firewall
- Lack of data backups
- Sharing of passwords
- Unsecure doors, windows

Step Four: Security Control Analysis – Analyze security controls already in place, such as log-ins, passwords, intrusion detection software and document tracking.

Step Five: Risk Likelihood Determination – After identifying potential threats and vulnerabilities, as well as the security controls the Practice currently has in place,

determine the probability that a vulnerability could be exploited by a threat.

- High – threat is capable, motivated, or likely and current security controls are ineffective.
- Medium – threat is capable, motivated, or likely, but security controls in place may prevent exploitation.
- Low – threat is not capable, motivated, or likely, or security controls in place will likely prevent exploitation.

Step Six: Impact Analysis – Determine the impact on the Practice that would result if a vulnerability was exploited by a threat. For example, you should consider the –

- Confidentiality of ePHI and the possibility of disclosure.
- Integrity of ePHI and the possibility of its alteration, loss or destruction.
- Availability of ePHI to authorized employees.

Step Seven: Risk Determination – Use the above information to identify the level of risk to ePHI and related information systems. The level of risk may be high, medium or low:

- High – security controls should be implemented as soon as possible.
- Medium – security controls should be implemented in a reasonable amount of time.
- Low – existing security controls are likely adequate or risk is acceptable.

Step Eight: Security Control Recommendations – Conclude the process by proposing security controls that can eliminate or mitigate the identified unacceptable risks to the confidentiality, integrity and accessibility of ePHI.

Step Nine: Documentation – After the above steps of the Risk Analysis have been completed, document the results in a written report. In addition, document the actions taken by the Practice to address any security problems you found, and the plans you have made to address security issues in the future.

Policies and Procedures. The HIPAA Security Rule requires that all covered health care providers have written policies and procedures. Those policies and procedures must address the 18 standards in the Security Rule, as well as the "required" and "addressable" implementation specifications for each standard.

This Manual contains policies and procedures that address each of the 18 standards in the Security Rule. This Manual is a template. Many of the policies in the Manual can be applied "as is" to your practice. For example, the policies in preceding sections B.1 and B.2 should apply to most practices and will require no modification.

Other policies in this Manual, however, are stated in general terms. As you consider the unique circumstances of your practice, you may wish to add more specifics; in some situations you may delete certain provisions that do not apply. For example, Section B.4 "Information Access Management," states that the Practice will protect ePHI from unauthorized access by keeping a log of computer passwords and keys to the Practice's building. You may determine in conducting your Risk Analysis, that these basic measures are insufficient to protect ePHI in your Practice. You may need to implement

a more complicated passwording system if you have multiple offices and numerous computer workstations. You may need to restrict the databases and programs on your computer system to limited Practice personnel. This is merely one example of the need to "customize" the basic policies and procedures in this Manual to your Practice. This will require thoughtful consideration by Practice personnel and may require outside technical expertise.

Risk Management. When you evaluate your Practice's security risks and implement policies and procedures to address those risks, you are engaging in the process of risk management. The purpose of risk management is to minimize legal liability and other adverse consequences that may occur if there is a breach of security to ePHI. Audits, investigations, lawsuits, loss of licensure, privileges and participation are all potential consequences of a security breach that results in improper disclosure of ePHI. The purpose of risk management is to prevent or reduce such adverse consequences. Implementing the policies and procedures in this Manual will be the foundation for your Practice's risk management efforts.

Enforcement of Policies and Procedures. Policies and procedures are meaningless if there is no commitment to uphold and enforce them. All Practice personnel must be trained to understand that the HIPAA Security Rule is federal law and that violating the provisions of this Manual could be harmful to the Practice and its patients. As a result, the Practice must enforce the policies in this Manual by disciplining personnel who fail to follow those policies. Mistakes or simple negligence will usually merit less severe discipline, especially for first-time offenses. Intentional security violations or repeated negligence will require more serious action, which may include termination.

Practice personnel should be encouraged to report security problems that they observe in the Practice. The Practice should never retaliate against anyone who provides such information, though discipline may have to occur for the violation itself.

Security incidents should be reported to the security officer. The security officer should document the incident, and, most importantly, the investigation of the cause of the problem and the steps taken to prevent it from recurring. The form found in Appendix F may be used for this purpose.

Proper security management will require ongoing review and monitoring by the security officer. At a minimum, such monitoring should include

- checking to see that daily backups of the computer system took place; and
- determining that no intrusions have occurred into either the Practice's physical facility or computer system.

These tasks can be performed by taking 10-15 minutes at the beginning of each work day. For example, the security officer could start his/her day by reviewing door locks and windows to ensure no intrusion into the Practice's office space; next the computer back-up could be checked from the previous night; finally, the Practice's anti-intrusion, virus protection and/or firewall software could be reviewed to determine whether any unauthorized access occurred.

4. Information Access Management

To the extent necessary and reasonable, the Practice will protect ePHI from unauthorized access by:

- Keeping a record of all past and present computer passwords of all Practice personnel; and
- Keeping a log of Practice personnel who have keys to Practice facilities.

Practice Guidance

In HIPAA terminology, "access" refers to the ability to create, read, modify or destroy ePHI. It is fundamental that only authorized and trusted individuals should have access to the ePHI of the Practice's patients.

One way to limit access is to properly manage the physical facilities in which computer systems are housed. This starts with access to the Practice's offices – whether such is a freestanding building, or simply a suite of offices in a larger structure. The primary issue here is keys or passcards that allow entry to office/building. A record should be kept of each person with an entry device (e.g., key, passcard). If possible, entry devices should be identified by number and a log kept of the person to whom that device is provided. Terminating employees must be required to return all access devices, and this should also be logged. The loss of keys or passcards should trigger action by the Practice such as changing locks or door codes.

Once steps are taken to secure the Practice's physical facilities, similar steps must be taken regarding access to the computer/information systems that reside within that physical facility. Just as a door and its lock allow access into the physical offices of the Practice, passwords allow access to computer and information systems. Those passwords, and the persons authorized to use them, must be logged. Records should be kept of both past and current passwords. When employees terminate, passwords must be changed and the new passwords recorded. The list of passwords must be kept in a secure manner and must be accessible in the event of an emergency.

5. Workforce Security

5.1 **Authorized Personnel.** Practice will only allow Practice personnel or other authorized individuals to access ePHI for legitimate purposes.

5.2 **Logoffs.** At the end of the day, all computer users must log off and/or shut down computers to prevent unauthorized disclosures.

5.3 **Minimum Necessary.** Practice personnel authorized to access PHI will only be authorized to access the minimum necessary ePHI to perform their job function. Access to any additional ePHI is prohibited.

5.4 **Departing Employees.** Precautions shall be taken to eliminate access to ePHI of Practice personnel whose employment is terminated. Such precautions may include, but are not limited to:

- Requiring the return of building/office keys, ID badges or access cards;
- Changing locks on building/office doors;
- Changing computer passwords;
- Requiring the return of laptop computers, PDAs, computer disks, etc.

Practice Guidance

Security professionals know that an organization's current and past employees are its most likely security risk. Unfortunately, employees may leave doors unlocked, may take Practice property out of the office, may disclose confidential information or maliciously destroy computer data. The Workforce Security policy above is designed to prevent or minimize such security breaches.

As a beginning point, only Practice personnel who have a legitimate need for access should be allowed access to patient ePHI. In a small office of two or three people, it is likely that all personnel will need to have full access. In a larger organization, however, such unlimited access may not be necessary or appropriate. Each practice must make this determination based on its own unique circumstances, but a conscious decision should be made.

For example, a practice may determine that its receptionist or "front office" personnel need access to computer billing information, but not to patient chart notes. Section B.5, above, could be amended to reflect this restriction and the security officer would ensure that front desk personnel did not have passwords or other access to the restricted information.

Terminating employees create special security concerns, especially when the termination occurs under less than amicable circumstances. The Practice should have established exit procedures that include the return of all Practice property,

especially keys, access cards, laptop computers and PDAs. Departing employees who refuse to return such items create a serious security vulnerability and the security officer must take responsibility to quickly address this problem by immediately changing locks, passwords, and in some circumstances, taking civil or criminal action to secure the return of computers or other devices containing patient ePHI.

The Practice should also recognize that its vendors and services providers (e.g. transcriptionists, software vendors, collection agencies) may have possession of ePHI of Practice patients, and that terminating employees may seek to gain access to that ePHI through these third parties. In some circumstances, then, it may be appropriate for the Practice to notify its vendors and service providers immediately that an employee has been terminated.

6. Security Incident Procedure

6.1 **Generally.** Practice personnel will report security incidents to the security officer.

6.2 **Respond to Security Incidents.** The Practice will respond to security incidents in an appropriate manner depending on the particular incident. This response will ensure that any damage that has occurred is minimized and corrected.

6.3 **Documentation.** Once the harmful effects of the incident have been mitigated, the security officer will document that incident in the Security Incident Tracking Report (see Appendix F for a sample report). This report will include the date and time of the incident, the type of incident and how it occurred, and all measures taken to remedy the breach and prevent similar breaches from recurring.

Practice Guidance

A "security incident" is a breach of security as to patient ePHI or the Practice's electronic information system or physical facility. Security incidents may include unauthorized access, use, modification or destruction of ePHI. A security incident may be as simple as leaving a door open overnight or sending an email to the wrong recipient; it may be more complicated, such as a virus that destroys or corrupts the Practice's electronic data.

Practice personnel should be trained to recognize security incidents and report them to the security officer. The security officer should, using Appendix F, investigate the incident and document the results of the investigation, including all remedial action taken to prevent such an incident recurring. Examples of remedial action may include employee discipline, additional training and education, upgrades or changes to computer systems and other similar measures.

Documentation of security incidents and the response to them is critical. Memories can fade and Practice personnel may come and go over the years. Without a permanent, written record of security issues and the corrective action taken, the Practice is more likely to fall repeatedly into the same problems, or waste time addressing issues that have already been corrected.

7. Emergency Plan

7.1 **Data Backup.** The Practice will create and maintain ePHI in duplicate form, such as paper copies, tape back-ups, CD-ROM or other external storage device (e.g. a "key or thumb drive"). A back-up copy should be kept both on- and off-site.

7.2 **Disaster Recovery.** The Practice will restore lost data caused by disasters or damage to the system.

7.3 **Emergency Mode Operation Plan.** The Practice will establish and implement, as needed, procedures to enable continuation of critical business processes of the Practice, as well as protection of the security of ePHI during and immediately after a crisis situation. This may require the backup of all systems or may only require the backup of critical programs, depending on the needs of the Practice.

Practice Guidance

An often forgotten component of a good security program is emergency or "contingency" planning. The loss or destruction of ePHI is a security incident and could result in significant harm to both the Practice and its patients. Emergencies that pose threats to ePHI may include natural disasters such as fire, flood, lightning strikes or earthquakes. Manmade situations such as riots, vandalism, theft and terrorism can also be emergencies that result in the loss or destruction of ePHI. A good emergency plan will include some basic procedures to protect the Practice and its electronic information.

As stated in the Security Rule:

> A contingency plan is the only way to protect the availability, integrity, and security of data during unexpected negative events. Data are often most exposed in these events, since the usual security measures may be disabled, ignored, or not observed.
>
> Without contingency planning, a covered entity has no assurance that its critical data could survive an emergency situation. Recent events, such as September 11, 2001, illustrate the importance of such planning. Contingency planning will be scalable based upon, among other factors, office configuration.

Perhaps the most basic emergency preparedness practice is having a back-up set of information. The Practice should maintain a duplicate of ePHI (and all other electronic data) that is kept off premises in a secure, accessible location. It is also a good idea to have a back-up copy onsite, if possible. This duplicate may be paper or electronic, depending on the Practice's particular

circumstances.

For example, a small practice with only one computer used for patient billing might print out its billing records on a weekly or monthly basis and keep this back-up copy at the officer manager's home or in a safety deposit box. A larger practice with several networked computers might have a tape back-up system that can be set to run each night. The office manager should take those back-ups home each night. Data could also be periodically downloaded onto CD-ROM, zip drives or "key drives" for purposes of having a back-up. The idea is to ensure that data is preserved if the Practice's physical facility or equipment are damaged or destroyed.

A second aspect of emergency planning is to have procedures in place to continue critical Practice functions, even in emergency situations. Having a back-up "copy" of ePHI is essential to continuity of patient care and billing operations, but other measures may also be needed. For example, if a fire destroyed the Practice's billing computer, the Practice could continue its billing operations by obtaining another computer if the Practice has (1) the software "master" and (2) an electronic or paper duplicate of the billing data. The same would be true with electronic patient records.

8. Evaluation

The Practice will periodically perform an evaluation of both technical (i.e. computers) and non-technical (i.e. door locks) security safeguards to determine compliance with the Security Rule. Evaluations must be performed any time there are environmental or operational changes that could affect the security of PHI.

Practice Guidance

Compliance with the HIPAA Security Rule, though not burdensome, will require ongoing monitoring and follow-up. The regulations specifically state that a Practice should periodically "evaluate" its security safeguards in order to ensure ongoing compliance. The regulations do not state how often this periodic evaluation must occur. As with most other aspects of the Security Rule, deciding how often to self-evaluate should be based on the size of the Practice and its electronic sophistication.

For example, a two- or three-person, single-office practice with one billing computer used for electronic billing could probably get by with annual or semi-annual evaluations. A larger practice with multiple locations and a networked information system, might need to do evaluations on a monthly or quarterly basis. Each practice should make this determination based on a review of its unique circumstances and in consultation with technical experts.

Larger practices may choose to have an outside consultant perform the periodic evaluations. The regulatory guidance from the government provides the following comment on this issue:

> Evaluation by an external entity is a business decision to be left to each covered entity. Evaluation is required under § 164.308(a)(8), but a covered entity may comply with this standard either by using its own workforce or an external accreditation agency, which would be acting as a business associate. External evaluation may be too costly an option for small entities.

Anytime your Practice makes a significant change to your computer or information system, an evaluation should be done to assess whether existing security measures remain adequate to protect ePHI. Significant changes might include the installation of new practice management and billing software, the purchase of new computer hardware, starting an Internet connection for the Practice or starting electronic billing in place of paper-only billing. These types of changes are referred to as "operational changes." The Security Rule also refers to "environmental changes," meaning changes in the physical surroundings in which your computer systems are located. For example, installing new computer hardware in a different part of your office building would be an environmental change that should prompt evaluation of security issues (e.g. door locks, fire hazards, etc.).

9. Disclosure to Business Associates

9.1 **Business Associates.** "Business associates" are third parties who provide services to the Practice and in so doing have access to electronic patient health information (ePHI). (Examples include: transcriptionists, billing services, clearinghouses, attorneys, accountants, collection agencies, etc. A more extensive definition may be found in Appendix G.)

9.2 **Requirement for Business Associate Agreements.** The Practice may disclose patient health information to its business associates only if the business associate has signed an agreement to (1) protect patient privacy by following HIPAA Privacy Rule, and (2) protect security of ePHI by following HIPAA Security Rule.

9.3 **Time for Obtaining New Business Associate Agreements.**

9.3.1 The Practice shall have its current business associates sign an agreement the same as or similar to that found in Appendix B prior to April 21, 2005.

9.3.2 Those business associates with whom the Practice forms a relationship after April 21, 2005, must sign an agreement the same or similar to that found in Appendix B. Patient health information may not be disclosed to business associates who fail or refuse to sign agreements by these dates.

9.4 **Existing Business Associate Agreements.** If the Practice currently has a business associate agreement in place, the Practice may execute the addendum found at Appendix C to add to their existing business associate agreement.

Practice Guidance

The HIPAA Privacy Rule defined business associates as third parties who provide services to the Practice and, in so doing, have access to patient health information. Most health care providers now have "business associate agreements" (BAA) in place with their service providers. The following are examples of those who are and are not business associates:

Are Business Associates	Not Business Associates
• Transcriptionists	• Other health care providers
• Billing services	• Insurance companies
• Collection agencies	• DME suppliers
• Software/hardware vendors	• Janitorial services
• Attorneys, accountants	• Plumbers, electricians

Under the Privacy Rule, the Practice must have a business associate agreement in place with a service provider if that service provider has access to PHI in written, oral or electronic form. By contrast, under the Security Rule, additional business associate agreement provisions are needed only if the service provider has access to ePHI.

For example, your Practice may employ a billing service and, in addition, a collection agency. Suppose hypothetically that electronic information is given to a billing service, but only paper records are given to the collection agency. Both service providers are business associates. As to the collection agency, the standard Business Associate Agreement in use under the Privacy Rule is sufficient because only paper PHI is provided. As to the billing service, however, a Business Associate Agreement with added Security Rule provisions is required because the Practice is providing ePHI.

For those practices that currently have a Business Associate Agreement in place with a service provider, a determination should be made as to whether ePHI is being provided to that business associate. If not, nothing more need be done. If ePHI is being provided, the Addendum to Business Associate Agreement found in Appendix C may be used to add the Security Rule provisions to the existing Business Associate Agreement.

If the Practice does not currently have any Business Associate Agreements in place with its service providers, and ePHI is being provided to them the full Business Associate Agreement found in Appendix B should be used.

The Practice should not allow its service providers to have access to ePHI unless and until a Business Associate Agreement (either Appendix B or C, as appropriate) has been signed.

The deadline for obtaining a signed Business Associate Agreement is April 21, 2005, so efforts should be made well in advance of that date to prepare and send out either Appendix B or C to the Practice's service providers. You may insert your Practice's name, the name of the service provider and other basic information into the blanks in Appendix B or C.

Section C: Physical Safeguards

1. Facility Access Controls

The Practice will limit unauthorized access to its building and offices, as well as to its information systems. The Practice will also ensure appropriate access by Practice personnel to ePHI.

Practice Guidance

Under the HIPAA Security Rule, your Practice has the responsibility to protect not only its electronic systems (e.g., computers), but also the building or office suite which houses those electronic systems. The single required specification under the Security Rule is that the Practice have reasonable procedures and safeguards in place to limit physical access to computers, while at the same time ensuring access to authorized Practice personnel.

At the most basic level, the Practice has the obligation to see that it has adequate doors, locks and other barriers that prevent physical intrusion into its offices by unauthorized persons. This might mean installing deadbolt locks or reinforced doors; in some urban locations, it may mean putting bars on windows or even having a security alarm system. Office sharing arrangements can create difficult problems, particularly when a co-tenant has unrestricted access to the Practice's offices.

If the Practice leases office space, the landlord should be consulted to ensure that the landlord restricts availability of access devices to the Practice's office space.

Inside the Practice's office, the Practice must have policies and procedures describing who has access to computer systems and how passwords are maintained and changed. The issue of patients, vendors, drug representatives and other visitors within the four walls of the Practice must also be addressed. Such visitors should be escorted and supervised at all times when they are on the Practice's physical premises.

The Practice should also address the following issues, and determine whether policies and procedures are needed:

- In an emergency situation, would access to the Practice's computer system be secure? Likewise, would Practice personnel be able to access computer systems in an emergency such as a flood, fire or earthquake?

- Is there a way to document repairs and modifications to the Practice's physical facilities in order to establish what has been done to correct physical access vulnerabilities?

2. Computer Workstation Use and Security

2.1 **Minimum Necessary.** Computer workstation access will be limited to those individuals who are authorized to use the workstation. For computer workstations used by more than one person, or where multiple Practice computers are part of a network, access by Practice personnel will be limited to those programs and databases applicable to the specific job duties of Practice personnel.

2.2 **Log Off.** Employees must log off of a computer before leaving it unattended for an extended period of time, including at night. Computers connected to the Internet or any other online connection should be turned off at the end of each work day.

2.3 **Physical Surroundings.** The physical surroundings of computer workstations will be arranged in a way that promotes security and avoids inadvertent, unauthorized access to ePHI.

Practice Guidance

There are two basic security requirements as to the Practice's individual computer workstations. First, Practice computers should only be used by personnel with a legitimate reason to do so. Second, as to those computers which Practice personnel are authorized to use, there must be appropriate restrictions as to the programs and data located on those computers. The policies set forth above are designed to satisfy these minimal standards in the Security Rule.

For example, suppose a small practice has two computer workstations, one located at the reception desk, the other in the back office. The front desk computer has basic patient scheduling and account information. The back office computer has more detailed billing and patient charting programs. In some practices, there may be a legitimate need for all personnel to have access to each computer and all data found on those computers. In other practices, however, it may be that the receptionist would not need to see or use the electronic billing software or the charting software. In such practices, there should be restrictions (particularly passwords) that prevent front desk personnel from accessing the billing and charting computer.

Obviously, having passwords is ineffective if computers are always left on without logoffs at night or when the authorized user(s) are away from that workstation for an extended period of time. Most computers today (those with Windows XP, Windows 2000 or Windows NT) have an automatic log-off or "screensaver" feature which can be set to blank out the computer screen and require a new login when the computer has not been used for a certain period of time.

Finally, computer monitors should be placed in appropriate locations with the screen facing an appropriate direction so as to minimize unauthorized viewing of the information on the screen.

3. Device and Media Controls

3.1 **Disposal.** When disposing of hardware or electronic media on which ePHI is stored, the data must be destroyed or deleted prior to disposal.

3.2 **Media Reuse.** Any electronic media that is being reused must be erased of all PHI prior to that reuse.

3.3 **Movement of Information Systems.** The Practice will document the receipt or removal of all computer hardware and electronic media that contain ePHI. The Practice will also document the destruction or deletion of ePHI when disposing of such hardware and electronic media.

Practice Guidance

The Security Rule requires the Practice to take certain steps to protect ePHI that may be found on Practice hardware and software, as well as the media (such as floppy disks, CD-ROMs and hard drives) that contain ePHI.

First, whenever computers or media are disposed of, this must be done in a way that permanently destroys the data contained therein (or prevents future access to that data). For example, some technical experts recommend cutting, shredding or incinerating floppy disks and CDs; they also suggest removing hard drives from computers and crushing the hard drive.

Second, if media is to be re-used, data should be deleted before such re-use occurs. For example, if floppy disks are to be re-used to send data to a transcriptionist or billing service, the floppy disk should be reformatted to delete all of the "old" data it may have had.

Third, the Practice should keep an "inventory" of its hardware and software. This inventory should track and record the acquisition of new hardware (computers, laptops, etc.) as well as software (master program disks and drivers). In addition, there should be a record of the disposition of hardware and software disposed of by the Practice.

Following the above procedures will help incidents such as those highly publicized debacles in which a hospital's or clinic's discarded computers (given away to charities or other organizations) were found to contain private patient information. It is not uncommon for a small practice to box up its old computers and put them into storage, with those computers years later going to the landfill or a charitable organization. Following the policies and procedures set forth above will ensure that those old computers do not come back to haunt the Practice.

Section D: Technical Safeguards

1. Access Controls

1.1 **Authorized Persons.** Only authorized persons will be allowed access to electronic information systems that store ePHI.

1.2 **User Identification.** All Practice personnel must be assigned a unique user name and/or number for identifying and tracking their identity in the electronic information system. Practice personnel cannot share the same password.

1.3 **Emergency Access Procedure.** In the event of an emergency, such as a power outage caused by natural and/or manmade disasters, ePHI that is essential for the continuation of patient care must be accessible. There should be one master password list (kept by the office administrator or similarly situated person) that will enable access to any system containing protected health information. This password should also serve to shut down the system in the event of a disaster.

Practice Guidance

Prior policies in this Manual have addressed the need to determine who has access to computers and databases in those computers. This policy provides further guidance on the issue of access by requiring that each computer user have his/her own unique user name and/or password. By "unique" it is intended that Practice personnel should not share or borrow the password of another employee.

Another dimension of access is ensuring that authorized personnel have access even in emergency situations, such as natural or manmade disasters. The Security Rule state:

> For example, in a situation when normal environmental systems, including electrical power, have been severely damaged or rendered inoperative due to a natural or manmade disaster, procedures should be established beforehand to provide guidance on possible ways to gain access to needed electronic protected health information.

There should always be a master set of passwords, recorded and maintained in the event of an emergency, such as the death or injury of an office manager. There should also be some type of emergency shutoff mechanism to prevent unauthorized access in times of emergencies. Screensavers that require a new log-in when the computer has not been used for a certain period of time are now common features on most computers.

Practices that use the Internet extensively, to convey ePHI, should also consider encryption. Encryption refers to the use of algorithms to encode and then

decode electronic data, so that only the intended receiver is able to read it. Encryption technology has made great strides in recent years but is probably not practical for most small practices at this time. Larger practices with extensive Internet transmissions and which are technically sophisticated should strongly consider encryption.

2. Audit Controls

The Practice will implement mechanisms to record and examine activity in information systems that include ePHI. The particular auditing mechanism should be appropriate to Practice needs and circumstances as determined by the Practice's risk analysis.

Practice Guidance

Most modern computer operating systems (Windows XP, Windows 2000, etc.) have the ability to track, or "audit" all those who log on or access a computer. With many systems, users can be tracked by their password as well as the programs accessed by the user. The date, time and extent of access may also be tracked. The Practice may use such auditing features to ensure that unauthorized personnel are not accessing ePHI. Auditing may also detect improper intrusions by hackers, ex-employees or others.

For many practices, some technical assistance may be needed in order to properly audit their computer systems. Such auditing should be done on a regular basis, either daily or weekly.

3. Integrity of ePHI

The Practice will protect ePHI from improper alteration or destruction by means of security software, if such is reasonable and necessary.

Practice Guidance

A key element of security is protecting data from unauthorized or improper alteration or destruction. The primary concerns here are viruses, hackers and disgruntled current or former employees. The loss or destruction of patient information could seriously impair patient care and expose the Practice to liability. The loss of billing data could result in catastrophic financial loss.

Several basic steps can be taken to reduce risks in this area. For practice computers that are connected to the Internet, virus protection software should be installed and updated regularly. In addition, a robust firewall should be installed to prevent intrusion by hackers or other unauthorized persons.

For computers not connected to the Internet, the integrity risks are primarily from internal sources, particularly Practice personnel. There are two primary means of reducing this risk. First, performing regular backups is essential to maintaining the integrity of ePHI in that lost or altered data can be easily restored. Second, the use of auditing programs can detect unauthorized access and identify changes to data.

Many electronic medical record programs today have features that protect the integrity of ePHI. For example, some of these programs will not allow certain types of entries to be made (e.g. ordering a prescription for drugs) unless the user has the requisite authorization on the system. Further, once an entry has been "finalled," either through an electronic signature or otherwise, the entry cannot be altered or deleted. These features are highly effective in preserving the integrity of Practice data.

4. Person or Entity Authentication

Prior to allowing access to ePHI, the Practice will verify the identity of any person or entity seeking such access.

Practice Guidance

The HIPAA Security Rule requires that health care providers implement procedures to verify the identity of those, both inside and outside the Practice, who seek access to ePHI. For Practice employees in small practices with just one or two computers, utilizing a username of four to six characters and a password of four to six characters would be appropriate, along with automatic logoff features activated on these computers. For larger practices with networked computer systems, access to ePHI utilizing a username of six to eight characters along with a strong password would be appropriate. A strong password is typically six to eight characters in length with a mixture of upper and lower case letters as well as numbers.

In addition, when transmitting ePHI electronically, the identity of the receiver should be verified before the transmission.

5. Transmission Security

The Practice will guard against unauthorized access to ePHI transmitted over an electronic communications network.

Practice Guidance

Transmission security has to do with the security of ePHI as it is being sent from one electronic device to another. With today's technology, transmission may occur in various ways: via dial-up access to a single, secure telephone number (e.g. Medicare billing); via dial-up Internet connection (typically with a 56k modem); via high speed Internet connection (e.g. using DSL, cable or T-1 line); or via wireless connection.

For many small practices, their only electronic transmissions are for billing purposes using a direct dial-up connection either to Medicare or a private payor. For such practices, transmission security will present little if any risk of unauthorized access to ePHI. The Preamble to the HIPAA Security Rule confirms this:

> We agree with the commenters that switched, point-to-point connections, for example, dial-up lines, have a very small probability of interception.

Transmission of ePHI over the Internet presents serious security risks, and should be avoided unless certain precautions are taken. The best, and only complete, protection for ePHI transmitted over the Internet is the use of encryption software. Such software electronically "scrambles" or codes electronic information, such as an email, so that an unauthorized person cannot read it. The receiver of the email must have the ability, however, to unscramble or decode the email with its own encryption software. At this time, encryption is not a practical or feasible option for most health care providers, particularly small providers.

If Internet transmission cannot be avoided, some basic steps should be taken to ensure the security of those transmissions. For example, the Practice should seek to verify email addresses and other recipient information prior to a transmission. In addition, the Practice should place a confidentiality statement in the "header" of any electronic document that is transmitted. This header could state the following:

> This email contains confidential health information and is intended only for the use of the individual or entity to which it is addressed. If you have received this communication in error, please do not

distribute it. Please notify the sender by email at the address shown and delete the original message.

Finally, if ePHI is to be transmitted via the Internet, such should only be done to a secure website (e.g. insurance payor's website or a clearinghouse website).

6. Record Retention and Disposal

6.1 **Policies and Procedures Maintained.** The Practice will keep and maintain written policies and procedures that reflect its compliance with HIPAA Security Rule.

6.2 **Document Retention Period.** The Practice will retain, for a minimum of six (6) years, all records, documents or information that is generated, created or required to be kept under the policies and procedures in this Manual, or as otherwise required by the HIPAA Security Rule. The six-year period shall run from the date the record was prepared, or the date it was last in effect, whichever is later.

6.3 **Storage in Secure Locations.** Electronic PHI of the Practice will be kept or stored in safe, secure locations. Computers or other electronic equipment or media that are stored offsite will be placed only in secure facilities.

Practice Guidance

Every practice should have written policies and procedures designed to ensure compliance with HIPAA. This Manual contains the basic policies, procedures and forms that a health provider needs for compliance with the HIPAA Security Rule. Some of the policies contained in the Manual are necessarily general; additional specificity and detail may be needed in your Practice based upon your particular circumstances.

You should retain all compliance documentation (e.g., Business Associate Agreements, Risk Assessments, evaluations, security incident reports, etc.) for at least six years from the creation of the document, or the date on which it was last in effect, whichever is later.

To the extent that you store computers or other electronic equipment or media offsite, only secure, reliable storage facilities should be used – preferably a bonded warehouse or storage facility.

APPENDICES

A. Risk Analysis Checklist

B. Business Associate Agreement

C. Addendum to Business Associate Agreement

D. Security Training and Education Log

E. Practice Resolutions

F. Security Incident Tracking Report

G. Glossary of Terms

H. HIPAA Resources

I. Acknowledgment of Receipt/Review of HIPAA Security Manual

J. Security Manual Checklist

APPENDIX A

Risk Analysis Checklist

RISK ANALYSIS CHECKLIST

The following risk analysis should be completed for your Practice. Thinking about and answering these questions will help you recognize security issues in your Practice. Completing this checklist will also help you in customizing this Manual to the particular circumstances of your Practice.

A. General Information

1. Inventory of computer and electronic hardware owned or used by the Practice

- List by name and model each computer owned/used by the Practice: _____ _____ _____ _____

- List by name and model all laptop computers, personal digital assistants (PDAs) or other portable electronic devices or equipment owned/used by the Practice. _____ _____ _____ _____

- List all printers and facsimile machines owned/used by the Practice. _____ _____ _____ _____

- List by name, address and telephone numbers all vendors or service providers who maintain the above-listed hardware. _____ _____ _____ _____

- For all hardware listed above, does the Practice have the drivers and master operating system disks? Yes ☐ No ☐

    - Where are these kept? _____ _____

2. Inventory of practice software

- For each computer or laptop listed above, state the operating system (e.g. Windows XP, windows 2000) it uses. _____ _____ _____ _____

- List each software program currently owned or used by the Practice (include billing, practice management, virus protection, firewall, charting, word processing and spreadsheet programs). _____ _____ _____ _____

- List passwords or codes, if any, needed to access the above-listed software programs. _____ _____ _____ _____

- For each software program listed above, state whether it has been upgraded and the date of the upgrade. _____ _____ _____ _____

- For each software program listed above, does the Practice have the master software disks? Yes ☐ No ☐

    - Where are these kept? _____ _____

    - Are all software licenses current? Yes ☐ No ☐

- List by name, address and telephone number your software vendors and service providers. _____ _____ _____ _____

3. Networks

- Are your Practice computers connected via a Local Area Network (LAN) or some other network system? Yes ☐ No ☐

If so, what type of network hardware and software do you have? _____
_____
_____
_____

- List name and type of server hardware. _____
_____
_____

4. Online Transmission and Access

- Does your Practice transmit any information electronically? Yes ☐ No ☐

  If so, is this done via:

  ☐ dial-up telephone connection for billing purposes (e.g. Medicare billing)?
  ☐ dial-up Internet connection?
  ☐ high speed Internet connection (e.g. DSL, cable, T-1 line)?
  ☐ wireless access?

- Can Practice personnel access your computer system from remote locations? Yes ☐ No ☐

  If so, is this done via:

  ☐ dial-up modem/Internet?
  ☐ high speed Internet?
  ☐ wireless access?

5. Emergency and Security

- Where does the Practice keep backup tapes or disks? _____
_____

- Does the Practice have:

  ☐ an Emergency Power Supply (EPS)?
  ☐ surge protectors?
  ☐ smoke alarms and fire extinguishers?
  ☐ security alarm system for building or office suite?

Note: The following are yes/no questions that correspond with the Security Rule standards and the sections of this Manual. A "no" answer suggests a security deficiency.

B. Administrative Safeguards

1. Personnel Designations. The Practice has appointed a security officer. Yes ☐ No ☐

2. Security Awareness and Training

- The security officer has received training regarding the HIPAA Security Rule. Yes ☐ No ☐
- Practice employees have been trained regarding the Practice's security policies and procedures. Yes ☐ No ☐
- The Practice has documentation reflecting the training of all employees (documentation shows date, content of training and name of employee). Yes ☐ No ☐

3. Security Management

- The Practice has done a security risk assessment. Yes ☐ No ☐
- The Practice has written security policies and procedures. Yes ☐ No ☐
- All door keys or other access devices are accounted for. Yes ☐ No ☐
- Practice employees who violate security policies and procedures receive appropriate educational/disciplinary action. Yes ☐ No ☐
- Practice employees are encouraged to report security incidents to the security officer. Yes ☐ No ☐
- The Practice's response to security incidents is documented. Yes ☐ No ☐

- The Practice's security officer (or another employee assigned by her/him) regularly reviews information system activity for possible security incidents. Yes ☐ No ☐

4. Information Access Management

- The Practice has a list of all past and current information system or computer passwords. Yes ☐ No ☐
- The Practice keeps a log of all employees with keys, passcards or other access devices to the Practice's building or office suite. Yes ☐ No ☐
- Door keys are "Do Not Duplicate"-type keys. Yes ☐ No ☐

5. Workforce Security

- Only authorized Practice personnel are permitted to have access to ePHI. Yes ☐ No ☐
- Authorized Practice personnel only have access to the minimum necessary ePHI for their job duties. Yes ☐ No ☐
- Computer users log off their computers at the end of the day. Yes ☐ No ☐
- Terminating employees are required to return keys, passcards and other access devices. Yes ☐ No ☐
- Terminating employees are required to return Practice laptops, PDAs, cellphones or disks. Yes ☐ No ☐
- Passwords are changed on computers when an employee leaves the Practice. Yes ☐ No ☐

- If terminating employees fail to return keys or other Practice property, action is taken to prevent improper use or disclosure of ePHI (changing door locks, filing police reports, etc.). Yes ☐ No ☐

6. Security Incident Procedures

- The Practice responds appropriately to security incidents by investigating and taking corrective action. Yes ☐ No ☐

7. Emergency Planning

- The Practice keeps a duplicate copy (paper or electronic) of all ePHI. Yes ☐ No ☐
- Backup copies of ePHI are updated regularly. Yes ☐ No ☐
- Backup copies are kept off-site at a location known to Practice personnel. Yes ☐ No ☐
- The Practice could, in the event of an emergency (fire, flood, earthquake) restore ePHI that is lost or damaged. Yes ☐ No ☐
- The Practice could, in the event of an emergency, ensure access by Practice personnel to ePHI. Yes ☐ No ☐
- The Practice keeps off-site, or in a fireproof cabinet on-site, copies of software master disks and hardware drivers. Yes ☐ No ☐
- The Practice has an emergency plan for restoring lost data and continuing business and patient care operations. Yes ☐ No ☐
- The Practice has an Emergency Power Supply (EPS) for server computers. Yes ☐ No ☐

8. Evaluation

- The Practice evaluates its security risks each time it –

  - upgrades or installs software — Yes ☐ No ☐
  - obtains new computer hardware — Yes ☐ No ☐
  - moves to a new office facility — Yes ☐ No ☐
  - connects to the Internet or establishes another online connection — Yes ☐ No ☐
  - makes some other significant change to its computer system — Yes ☐ No ☐

9. Business Associates

- Does the Practice provide ePHI to vendors or service providers (e.g. transcriptionists, billing services, collection agencies)? If so,

  - Does the Practice have a Business Associate Agreement in place with those parties? — Yes ☐ No ☐

C. Physical Safeguards

1. Facility Access Controls

- The Practice's office space is not shared with other health care providers. — Yes ☐ No ☐

- Building/office doors, filing cabinets and desks are locked at night. — Yes ☐ No ☐

- Building/office windows are secure and/or barred. — Yes ☐ No ☐

- The building/office has a security alarm system. — Yes ☐ No ☐

- Does the Practice escort patients, vendors and sales representatives in all back-office areas where ePHI is located? — Yes ☐ No ☐

2. Computer Workstation Security

- The Practice limits use of computers and software programs to employees who have a legitimate need for access to such. Yes ☐ No ☐
- Practice employees log off their computers at the end of each work day. Yes ☐ No ☐
- Practice employees turn off computers at the end of each work day. Yes ☐ No ☐
- Practice computers return to the logon screen automatically or have password-enabled screensavers that engage when computers are left inactive for any extended period of time. Yes ☐ No ☐
- Computer monitors are placed in such a way as to prevent viewing by unauthorized persons. Yes ☐ No ☐

3. Device and Media Controls

- The Practice removes or destroys ePHI on computer hard drives when disposing of computers. Yes ☐ No ☐
- The Practice erases or destroys electronic media (disks, tapes, CD-ROMs) that contain ePHI prior to disposal. Yes ☐ No ☐
- The Practice erases ePHI on electronic media that is to be re-used by the Practice. Yes ☐ No ☐
- The Practice has a written inventory of –
  - all electronic and computer hardware Yes ☐ No ☐
  - all software programs Yes ☐ No ☐
- The Practice documents (and keeps such documentation) the receipt, removal or disposal of hardware and electronic media. Yes ☐ No ☐

D. Technical Safeguards

1. Access Controls

- All Practice personnel are assigned unique user names and passwords. Yes ☐ No ☐
- Practice employees do not share passwords. Yes ☐ No ☐
- A master password list is maintained both onsite and offsite in locations known to Practice personnel. Yes ☐ No ☐
- User IDs and passwords are not posted on or near workstations. Yes ☐ No ☐
- Laptops, PDAs and other portable electronic equipment are kept physically secured with a lock when not in use. Yes ☐ No ☐
- Passwords are changed on a regular basis. Yes ☐ No ☐
- A history of previously used passwords is kept to prevent reuse. Yes ☐ No ☐

2. Audit Controls

- The Practice security officer routinely reviews computer audit logs to check for unusual or unauthorized access to ePHI by Practice employees. Yes ☐ No ☐
- The security officer routinely checks for intrusions from outside parties to Practice computer systems. Yes ☐ No ☐
- The Practice's computer system logs accesses and attempts by date, time, user ID and location. Yes ☐ No ☐
- The Practice keeps a log of all security maintenance by date and type of maintenance performed. Yes ☐ No ☐

3. Integrity of ePHI

- The Practice has virus protection software, which it keeps updated. Yes ☐ No ☐
- The computer system prevents alteration of "final" or "signed" documents. Yes ☐ No ☐
- For computers connected to the Internet, the Practice has a firewall. Yes ☐ No ☐
- The Practice does regular backups of its electronic data. Yes ☐ No ☐
- The Practice regularly audits its user login profiles. Yes ☐ No ☐
- All Practice computers have surge protectors. Yes ☐ No ☐
- The Practice has smoke alarms and fire extinguishers. Yes ☐ No ☐

4. Person or Entity Authentication

- The Practice verifies the identity of those to whom it transmits ePHI. Yes ☐ No ☐

5. Transmission Security

- The Practice refrains from transmitting ePHI via the Internet, or only transmits ePHI to secure websites. Yes ☐ No ☐
- If the Practice transmits ePHI via the Internet, it uses encryption. Yes ☐ No ☐
- The Practice uses only secure dialup lines for purposes of transmitting ePHI electronically. Yes ☐ No ☐

6. Record Retention and Disposal

- The Practice retains, for a minimum of six years, all HIPAA compliance documentation. Yes ☐ No ☐
- Computers and electronic media are disposed of properly when discarded by the Practice. Yes ☐ No ☐
- Computers and electronic media are stored in secure facilities. Yes ☐ No ☐

APPENDIX B

Business Associate Agreement

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (Agreement) is made and entered into by and between _____ **[insert name of Practice]** and **_____ [insert name of Business Associate]** on this _____ day of _____, 200__. In consideration of the mutual covenants contained in this Agreement and intending to be legally bound, the parties agree as follows:

1. Definitions:

Business Associate. "Business Associate" shall mean _____ [Insert Name of Business Associate].

ePHI. "ePHI" shall mean Protected Health Information transmitted by or maintained in electronic media.

Practice. The "Practice" shall mean [Insert Name of Practice].

Patient. "Patient" shall have the same meaning as the term "individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR 164.501, as limited to the information created or received by Business Associate from or on behalf of Practice.

Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR 164.501.

Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

Security Incident. "Security Incident" shall mean a violation of the Security Rule, or the breach of confidentiality, integrity or accessibility of ePHI.

Security Rule. "Security Rule" shall mean the statutes for security of individually identifiable health information at 45 CFR part 164, subpart C.

2. Obligations and Activities of Business Associate

Business Associate agrees:

(a) Not to use or disclose Protected Health Information other than as permitted or required by the Agreement or as required by law.

(b) To use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

(c) To mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

(d) To report to Practice any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

(e) To ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Practice, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

(f) To provide access, at the request of Practice, and in the time and manner requested by the Practice, to Protected Health Information to the Practice or, as directed by Practice, to an Individual in order to meet the requirements under 45 CFR 164.524.

(g) To make any amendment(s) to Protected Health Information in a Designated Record Set that the Practice directs or agrees to pursuant to 45 CFR 164.526 at the request of Practice or a Patient, and in the time and manner requested by the Practice.

(h) To make its internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of Practice available to the Practice, or to the Secretary, in a time and manner requested by the Practice or designated by the Secretary, for purposes of the Secretary determining Practice's compliance with the Privacy Rule and Security Rule.

(i) To document disclosures of Protected Health Information and information related to such disclosures as would be required for Practice to respond to a request by a Patient for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

(j) To provide to Practice or a Patient, in time and manner requested by the Practice, information collected in accordance with subsection 2(i) of this Agreement, to permit Practice to respond to a request by a Patient for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

(k) To implement administrative, physical, and technical safeguards that reasonably and appropriately protect confidentiality, integrity and accessibility of the electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of the covered entity.

(l) To ensure that any agreement, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it.

(m) To report to Practice any security incident of which it becomes aware.

(n) To authorize termination of the contract by Practice, if Practice determines that the Business Associate has violated a material term of the contract.

(o) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic health information that it creates, receives, maintains, or transmits on behalf of the Covered Entity.

(p) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it.

(q) Report to the Covered Entity any security incident of which it becomes aware.

(r) Authorize termination of the contract by the Covered Entity, if the Covered Entity determines that the Business Associate has violated a material term of the contract.

3. Permitted Uses and Disclosures by Business Associate

[use one of the following versions]

Specific purposes: Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Practice for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule or Security Rule if done by Practice or the minimum necessary policies and procedures of the Practice: _____
_____
_____
[List Purposes].

<or>

Underlying services agreement: Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities or services for, or on behalf of, Practice as specified in the agreement with _____ **[Insert Name of Business Associate]**, provided that such use or disclosure would not violate the Privacy Rule or Security Rule if done by Practice or the minimum necessary policies and procedures of the Practice.

4. Obligations of the Practice

Practice shall:

(a) Notify Business Associate of any limitation(s) in its notice of privacy practices of Practice in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

(b) Notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

(c) Notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Practice has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

5. Permissible Requests by Practice

Practice shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule or Security Rule if done by Practice.

6. Term and Termination

(a) Term: This Agreement shall be effective as of _____ **[Insert Effective Date]**, and shall terminate when all of the Protected Health Information provided by Practice to Business Associate, or created or received by Business Associate on behalf of Practice, is destroyed or returned to Practice, or, if it is impractical to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

(b) Termination for Cause: Upon Practice's knowledge of a material breach by Business Associate, Practice shall either: (1) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement and any related agreement if Business Associate does not cure the breach or end the violation within the time specified by Practice; (2) Immediately terminate this Agreement and any related agreement entered into by the parties if Business Associate has breached a material term of this Agreement and cure is not possible; or (3) If neither termination nor cure are feasible, Practice shall report the violation to the Secretary.

(c) Effect of Termination:

(1) Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Practice, or created or received by Business Associate on behalf of Practice. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(2) In the event that Business Associate determines that returning or destroying the Protected Health Information is impractical, Business Associate shall provide to Practice notification of the conditions that make return or destruction impractical. Upon providing notice that return or destruction of Protected Health Information is impractical, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction impractical, for so long as Business Associate maintains such Protected Health Information.

7. Miscellaneous

(a) Regulatory References: A reference in this Agreement to a section in the Privacy Rule or Security Rule means the section as in effect or as amended.

(b) Amendment: The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Practice to comply with the requirements of the HIPAA Privacy Rule or Security Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

(c) Survival: The respective rights and obligations of Business Associate under subsection 4(c) of this Agreement shall survive the termination of this Agreement.

(d) Interpretation: Any ambiguity in this Agreement shall be resolved to permit Practice to comply with the HIPAA Privacy Rule or Security Rule.

8. Indemnification

Business Associate shall defend and indemnify the Practice from and for any and all liability, claims, proceedings, suits, damages, or causes of action resulting in any way from Business Associate's breach of this Agreement or breach of the HIPAA Privacy Rule or Security Rule. The duty to indemnify shall include the duty to defend the Practice by hiring competent legal counsel at Business Associate's expense.

The parties have caused this Agreement to be executed on the date first written above.

[Insert name of Practice]	**[Insert name of Business Associate]**
By:_____	By:_____
Its:_____	Its:_____

APPENDIX C

Addendum to Business Associate Agreement

ADDENDUM TO BUSINESS ASSOCIATE AGREEMENT

This Addendum to the Business Associate Agreement between _____ **[insert name of Practice]** ("Covered Entity") and _____ **[insert name of Business Associate]** ("Business Associate") is entered into this _____ day of _____, 200__. This Addendum hereby amends the Business Associate Agreement dated _____, 200__.

1. Additional Definitions

ePHI. "ePHI" shall mean Protected Health information transmitted by or maintained in electronic format.

Security Incident. "Security Incident" shall mean a violation of the Security Rule, or the breach of confidentiality, integrity or accessibility of ePHI.

Security Rule. "Security Rule" shall mean the statutes for security of individually identifiable health information at 45 CFR part 164, subpart C.

2. Additional Duties and Obligations of Business Associate

As set forth in the HIPAA Security Rule, 45 CFR part 164, subpart C, Business Associate will:

1. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic health information that it creates, receives, maintains, or transmits on behalf of the Covered Entity;

2. Ensure that any agent, including a subcontractor, to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect it;

3. Report to the Covered Entity any security incident of which it becomes aware; and

4. Authorize termination of the contract by the Covered Entity, if the Covered Entity determines that the Business Associate has violated a material term of this Addendum.

The parties have caused this Addendum to be executed on the date set forth above.

[Insert name of Practice]	**[Insert name of Business Associate]**
By:_____	By: _____
Its:_____	Its: _____

APPENDIX D

Security Training and Education Log

Security Training and Education Log

Date of Training	Name of Employee	Description of Training	Training Hours	Person/Company Providing Training

APPENDIX E

Practice Resolutions

PRACTICE RESOLUTION
ADOPTION OF HIPAA SECURITY MANUAL

WHEREAS, _____ **[insert name of Practice]** ("the Practice") has authorized the preparation of a HIPAA Security Manual; and

WHEREAS, the Practice has reviewed the Security Manual; and

WHEREAS, the Security Manual is intended to satisfy fully the requirements set forth in the federal HIPAA Security Rule;

NOW THEREFORE,

BE IT RESOLVED, that the Practice hereby approves of the adoption of the HIPAA Security Manual, effective _____ **[insert date]**, with the expectation that all Practice employees, including those with an ownership interest in the Practice, will be instructed in their respective duties under the Manual and will comply fully therewith.

Date:_____

By:_____
[insert name of authorized signer]

PRACTICE RESOLUTION
APPOINTMENT OF A SECURITY OFFICER

WHEREAS, _____ **[insert name of Practice]** ("the Practice"), having approved the adoption of the HIPAA Security Manual; and

WHEREAS, the Security Manual requires the appointment of a Security officer; and

WHEREAS, the Practice having great confidence in the integrity, experience, and judgment of _____ **[insert name of Security officer]**;

NOW THEREFORE,

BE IT RESOLVED, that the Practice does hereby appoint _____ **[insert name of Security officer]** to be the Security officer of the Practice beginning _____ **[insert date]**, and continuing until changed in accordance with the HIPAA Security Manual; and

BE IT FURTHER RESOLVED, that the Security officer will vigorously carry out the duties set forth in the Security Manual and that all employees of the Practice will be informed of the importance of adherence to the Security Manual and the importance of their cooperation with the Security officer.

Date:_____

By:_____
[insert name of authorized signer]

APPENDIX F

Security Incident Tracking Report

Security Incident Tracking Report

Date: _____

Time: _____

Description of Security Incident:

_____

_____

_____

_____

Measures Taken to Mitigate Effects and Resolve Problem:

_____

_____

_____

_____

Steps Taken to Prevent Recurrence:

_____

_____

_____

_____

_____

Signature of Security Officer

APPENDIX G

Glossary of Terms

GLOSSARY OF TERMS

Access – The ability or the means necessary to read, write, modify or communicate data/information or otherwise use any system resource.

Administrative safeguards – Administrative safeguards are the policies and procedures the Practice implements to execute the physical and technical safeguards. There are nine components of administrative safeguards in the Security Rule: (1) security management (includes performance of risk analysis, risk management, preparation of sanction policy and monitoring computer systems activities); (2) assignment of a security officer; (3) a system administrator; (4) management of the access of information; (5) security training; (6) incident reporting and investigation; (7) implementation of a contingency plan; (8) periodic evaluation of technology and upgrades; and (9) business associate agreements in place to protect ePHI.

Authentication – The corroboration that a person is the one claimed.

Availability – The property that data or information is accessible and useable upon demand by an authorized person.

Business associate – A person who on behalf of a covered entity (or of an organized health care arrangement in which the covered entity participates) performs, or assists in the performance of:

- A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
- Any other function or activity regulated by this subchapter; or
- A person who provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity (or to or for an organized health care arrangement in which the covered entity participates) where the provision of the service involves the disclosure of individually identifiable health information from such covered entity (or arrangement), or from another business associate of such covered entity (or arrangement), to the person.

Confidentiality – The property that data or information is not made available or disclosed to unauthorized persons or processes.

Covered entity – (1) A health plan (includes insurance companies, Medicare, Medicaid, group health plans, etc.); (2) a health care clearinghouse; or (3) a health care provider who transmits any health information in electronic form in connection with a standard HIPAA transaction (such as electronic billing).

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

Electronic media – Includes memory devices in computers (hard drives) and any removable/transportable digital memory medium.

Electronic Protected Health Information (ePHI) – Individually identifiable health information transmitted by electronic media or maintained in electronic media.

Encryption – 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.

Facility – The physical premises and interior and exterior of a building in which ePHI is located.

HHS or Secretary – The Department of Health and Human Services or the Secretary of Health and Human Services.

Health care – Care, services, or supplies related to the health of an individual. *Health care* includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care provider – A provider of services (as defined in Section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of protected health or health services (as defined in Section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information – Any information, oral or recorded in any medium, that:

- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Individually identifiable health information – Information that is a subset of health information, including demographic information collected from an individual, and that: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) Which

identifies the individual, or (ii) With respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Information system – An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity – The property that data or information have not been altered or destroyed in an authorized manner.

Minimum necessary – When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Payment – Any of a number of activities by a covered entity involving reimbursement or coverage related to health care or health benefits. The definition of payment includes: obtaining premiums or identifying or providing benefits under a health plan; reimbursement for health services, determining eligibility, coverage, adjudication, or subrogation of health benefit claims; risk adjusting amounts due based on enrollee health status and demographics; billing, claims management, collection activities, obtaining payment under a contract for reinsurance and related health care data processing; review of health care services for protected health necessity, coverage under a health plan, appropriateness of care, or justification of charges; utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services; and disclosure to consumer reporting agencies of certain protected health information relating to collection of premiums or reimbursement (i.e., name and address, date of birth, social security number; payment history; account number; and name and address of the health care provider and/or health plan).

Physical safeguards – Physical safeguards are the security measures that protect the physical facility and computer systems. There are four components of physical safeguards in the Security Rule: (1) facility access controls (locks, screen filters, magnetic cards); (2) workstation use; (3) workstation security; and (4) device and medical controls (disposal, reuse, accountability and backup storage).

Protected health information – Individually identifiable health information that is or has been electronically maintained or electronically transmitted by a covered entity, as well as such information when it takes any other form that is (1) Created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. Protected health information excludes individually identifiable health information in employment records held by a covered entity in its role as an employer.

Required by law – A mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. *Required by law* includes, but is not limited to, court orders and court- ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Security incident – A violation of security policies and procedures. A security incident includes the attempted or successful unauthorized access, use, disclosure, modification or destruction of information, or interference with the operation of an information system. Examples: An unauthorized person accesses ePHI, a door is left unlocked, a hacker gets into the system. All security incidents must be documented.

Security officer – The individual designated by a health care provider to develop and implement security policies and procedures for the provider.

Technical safeguards – Technical safeguards and those electronic and computerized security measures installed (such as passwords) to protect information contained in the facility and computer system. There are five components of technical safeguards in the Security Rule: (1) access control (password encryption); (2) audit control; (3) integrity controls; (4) authorization; and (5) transmission security.

Treatment – The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

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

Workforce – Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Workstation – An electronic computing device, such as a desktop or laptop computer, personal digital assistant (PDA) or other similar electronic device.

APPENDIX H

HIPAA Resources

HIPAA RESOURCES

Helpful General and Government Websites

Listed below are some valuable resources on the Internet that provide general information about HIPAA and the HIPAA Security Rule:

- CMS HIPAA Site: http://www.cms.hhs.gov/hipaa/hipaa2/default.asp
- HHS Administrative Simplification: http://aspe.hhs.gov/admnsimp/index.shtml
- HIPAAlert: http://www.hipaadvisory.com/alert
- SNIP: http://snip.wedi.org
- WEDI: http://www.wedi.org
- OCR website: http://www.hhs.gov/ocr/hipaa
- National Institute of Standards and Technology (NIST) website: http://csrc.nist.gov
- Utilization Review Accreditation Commission (URAC): http://www.urac.org

APPENDIX I

Acknowledgment of Receipt/Review
of
HIPAA Security Manual

EMPLOYEE ACKNOWLEDGMENT OF RECEIPT/REVIEW

OF

HIPAA SECURITY MANUAL

I, _____, acknowledge that I have received and/or
(print full name)
reviewed the HIPAA Security Manual and that I will comply with its provisions. I acknowledge that failure to comply could result in disciplinary action, up to and including termination.

_____ _____
(Signature) (Date)

APPENDIX J

Security Manual Checklist

SECURITY MANUAL CHECKLIST

HIPAA requires health care providers to implement three types of security safeguards for ePHI: (1) administrative safeguards; (2) physical safeguards; and (3) technical safeguards. For each of these three types of safeguards, there are both "required" and "addressable" standards that must either be implemented or considered. "Required" means that the standard is not optional and must be implemented by the Practice. "Addressable" means that the Practice evaluate whether implementation is reasonable and appropriate in its particular circumstances. If it is appropriate and reasonable, it must be implemented; if not, the reasoning for such must be documented, and the Practice must implement an equivalent alternative measure if one is reasonable and appropriate.

Complete the checklist by reviewing the specifications accompanying each of the 18 standards set forth below. As to those items which you have completed (or which are not applicable), place a "check" in the box. Leave blank those items which remain to be completed.

ADMINISTRATIVE SAFEGUARDS

1. Personnel Designations.

Required	Addressable
□ Appoint a security officer	(None)

2. Security Awareness and Training of Practice Personnel.

Required	Addressable
□ Train Practice personnel regarding security awareness and the policies and procedures in the APMA HIPAA Security Manual.	□ Periodic security updates. □ Implement procedures for guarding against, detecting and reporting malicious software. □ Implement procedures to monitor login attempts and report discrepancies. □ Periodically change passwords and safeguard those passwords.

3. Security Management.

Required	Addressable
□ Conduct a risk analysis of potential threats and vulnerabilities to	(None)

confidentiality, integrity and accessibility.

- □ Implement security measures sufficient to reduce risks and vulnerabilities identified in the risk analysis.
- □ Implement discipline policy for practice personnel who fail to comply with security policies.
- □ Implement procedures to regularly review records of the activity of information systems containing ePHI.

4. Information Access Management.

Required	**Addressable**
(None)	□ Implement policies and procedures for granting access to ePHI, i.e. through access to workstation, program, transaction or process. □ Implement policies and procedures that establish, document, modify and review Practice personnel's access to ePHI.

5. Workforce Security.

Required	**Addressable**
□ Implement policies and procedures to ensure that only appropriate Practice personnel have access to ePHI.	□ Implement procedures for authorization and/or supervision of all personnel who may have access to ePHI. □ Implement procedures to determine appropriate access to ePHI. □ Implement procedures for preventing access to ePHI when the employment of a person is terminated.

6. Security Incident Procedures.

Required	Addressable
□ Identify and respond to suspected or known security incidents; mitigate harmful effects; document incident response and prevention of recurrence.	(None)

7. Emergency Plan.

Required	Addressable
□ Implement procedures to create and maintain duplicate versions of ePHI. □ Establish procedures to restore any loss of data □ Establish procedures to enable continuation of critical business processes for protection of ePHI while operating in emergency mode.	□ Implement procedures for periodic testing and revision of emergency plans □ Assess criticality of specific programs and data in support of other emergency plan components.

8. Evaluation.

Required	Addressable
□ Perform periodic technical and non-technical evaluations, to determine the overall effectiveness of the Practice's security practices and procedures.	(None)

9. Disclosure to Business Associates.

Required	Addressable
□ Sign business associate agreements or addenda with all business associates.	(None)

PHYSICAL SAFEGUARDS

1. Facility Access Controls.

Required	Addressable
□ Implement policies and procedures to limit physical access to computer systems while ensuring properly authorized access is allowed.	□ Establish procedures to allow facility access in the event of an emergency. □ Implement policies and procedures to safeguard the Practice's physical facilities and equipment therein. □ Implement procedures to control the access of people to the Practice's facilities and equipment. □ Implement policies and procedures to document repairs and modifications to the Practice's physical facilities.

2. Workstation Use and Security.

Required	Addressable
□ Implement policies and procedures that specify workstations to which Practice personnel are allowed access. □ Implement policies and procedures that specify those databases or programs to which Practice personnel are allowed access.	(None)

3. Device and Media Controls. Implement policies and procedures that govern the receipt or removal of hardware and electronic media that contain ePHI.

Required	Addressable
□ Implement policies and procedures to address proper disposal of hardware, or electronic media containing ePHI.	□ Maintain a record of the movement of hardware and electronic media and who is responsible for such.

□ Implement policies and procedures for removal of ePHI from electronic media before reuse.	□ Create a duplicate of ePHI before movement of equipment.

TECHNICAL SAFEGUARDS

1. Access Controls. Implement technical policies and procedures for computer systems that maintain ePHI to allow access only to authorized people.

Required	Addressable
□ Assign unique user identification to each employee. □ Establish emergency access procedure for obtaining necessary ePHI during the emergency.	□ Implement automatic logoff of computer workstations after a predetermined time of inactivity. □ Implement encryption and decryption devices for Internet transmittal of ePHI.

2. Audit Controls

Required	Addressable
□ Implement a mechanism to record and examine activity in systems that contain or use ePHI.	(None)

3. Integrity of ePHI

Required	Addressable
□ Implement policies and procedures to protect ePHI from improper alteration or destruction.	□ Implement electronic mechanisms to corroborate that ePHI has not been accessed, modified or destroyed in an unauthorized manner.

4. Person or Entity Authentication

Required	Addressable
□ Implement procedures to verify the identity of persons or entities seeking access to ePHI.	(None)

5. Transmission Security.

Required	Addressable
□ Implement technical security measures to guard against unauthorized access to ePHI transmitted over an electronic communications network.	□ Implement procedures to ensure electronically transmitted ePHI is not improperly modified. □ Implement mechanism to encrypt ePHI wherever appropriate.

6. Record Retention and Disposal.

Required	Addressable
□ Implement a record retention and disposal policy as to the Practice's compliance with the HIPAA Security Rule.	(None)