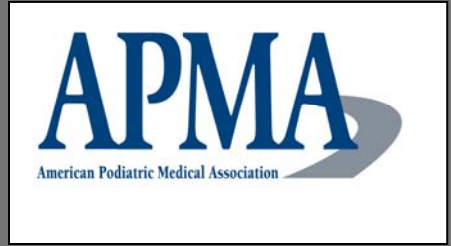


2010



HIPAA Security Manual

Revised with HITECH ACT Amendments

Authored by J. Kevin West, Esq.
© 2010 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 Rules 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 that may provide greater privacy protections. The provisions in this Manual may need to be modified to fit certain practitioners' specific individual circumstances. The publication of the APMA HIPAA Security Manual is intended for the use and benefit of APMA. The information and opinions presented herein may not reflect the official position of the APMA.

TABLE OF CONTENTS

INTRODUCTION.....	1
About this Manual.....	1
Who and What is Regulated by the Security Rule?	1
About the Author	1
Commonly Used Terms	2
POLICIES AND PROCEDURES	3
Section A: An Introduction to Basic Security Concepts and Compliance.....	4
1. Purpose of This Security Manual.....	5
2. Security Rule Concepts.....	6
Section B: Administrative Safeguards	7
1. Personnel Designations.....	8
2. Training of Practice Personnel.....	9
3. Security Management	10
4. Information Access Management	11
5. Workforce Security	12
6. Security Incident Procedure.....	13
7. Emergency Plan	14
8. Evaluation	15
9. Disclosure to Business Associates.....	16
10. Patient Notification of Breach of Protected Health Information	17
11. Technical Standards Published by the Federal Government Regarding Security of PHI	19
12. Record Retention and Disposal.....	20
Section C: Physical Safeguards.....	21
1. Facility Access Controls	22
2. Computer Workstation Use and Security	23
3. Device and Media Controls	24
Section D: Technical Safeguards	25
1. Access Controls	26
2. Audit Controls.....	27
3. Integrity of ePHI	28
4. Person or Entity Authentication.....	29
5. Transmission Security.....	30

APPENDICES..... 31

APPENDIX A.	Risk Analysis Checklist
APPENDIX B.	Business Associate Agreement
APPENDIX C.	Security Training and Education Log
APPENDIX D.	Practice Resolutions
APPENDIX E.	Security Incident Tracking Report
APPENDIX F.	Glossary of Terms
APPENDIX G.	HIPAA Resources
APPENDIX H.	Acknowledgment of Receipt/Review of HIPAA Security Manual
APPENDIX I.	Patient Notification of Unauthorized Disclosure

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). In February 2009, however, Congress passed the Health Information Technology for Economic and Clinical Health Act (HITECH Act). Most of the provisions in the HITECH Act took effect on February 17, 2010. The HITECH Act made significant changes to the HIPAA Security Rules and has necessitated the present revision to the APMA's 2004 Security Manual. This revised HIPAA Security Manual is intended to completely replace the prior version

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

About the Author

J. Kevin West is a partner with the firm of Hall, Farley, Oberrecht & Blanton, P.A. in Boise, Idaho. For over 24 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. For the past ten years, he has served as national counsel for the Podiatry Insurance Company of America (PICA) in supervising Medicare and other regulatory claims brought against PICA 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.

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 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 practice
Patient health information	“Protected Health Information,” as defined by HIPAA (see Glossary of Terms)
Electronic PHI or ePHI	“Protected Health Information,” maintained, created or transmitted in electronic format
Manual	This 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 This Security Manual

The general goal of this Security Manual is to:

- Ensure the confidentiality, integrity and availability of all ePHI that the Practice creates, receives, maintains or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of patient ePHI; and
- Ensure compliance by the Practice's workforce.

2. Security Rule Concepts

The HIPAA 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.

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).

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.

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 H 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 <insert date>. Training of employees hired after <insert date>, 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 C), 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 G).
 - Retained consultants and professional advisers.

Note: Practitioners are strongly encouraged to conduct a “refresher” training on the HIPAA Privacy Rules and include discussion of the new HITECH Act amendments.

3. Security Management

- 3.1 **Security Assessment of the Practice.** Using the Risk Analysis Checklist in Appendix A, the Practice and its counsel have conducted an accurate and thorough assessment of the current status of the Practice's security compliance to identify potential threats and vulnerabilities to the confidentiality, integrity and accessibility of ePHI held by the Practice.
- 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 E).
- 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.

4. Information Access Management

To the extent necessary and reasonable, the Practice will protect ePHI from unauthorized access by granting computer passwords only to personnel who have a legitimate need to see patient health information.

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.

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. If the security incident involves an unauthorized disclosure of PHI, the security officer will follow the patient notification procedure set forth in section A.10 of this Manual.
- 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 E 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.

Note: Because of the HITECH Act changes to HIPAA, new Business Associate Agreements should be executed with all business associates. The template found in Appendix B may be used for this purpose.

7. Emergency Plan

- 7.1 **Data Backup.** The Practice will create and maintain ePHI in duplicate form by means of a tape back-up system. The back-up copy will be kept either off-site or in a fireproof container on-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.

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.

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 F.)
- 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.** The Practice shall have all business associates sign an agreement the same as or similar to that found in Appendix B prior to <insert date>.

Note: Because of the HITECH Act changes to HIPAA, new Business Associate Agreements should be executed with all business associates. The template found in Appendix B may be used for this purpose.

10. Patient Notification of Breach of Protected Health Information

10.1 **General Rule.** If the Practice discloses unsecured PHI to an unauthorized person, or otherwise allows an unauthorized disclosure of unsecured PHI, the Practice must notify the affected patient(s), as set forth below. Unsecured PHI means health information that is not protected by technology that renders it unusable or unreadable to unauthorized persons.

10.2 Patient Notification Procedures

10.2.1 In the event of an unauthorized disclosure of unsecured PHI, affected patients must be notified in writing by first class mail. If the Practice does not have current mailing information, notice may be given by telephone or email.

10.2.2 If the Practice does not have current contact information on ten (10) or more patients affected by the unauthorized disclosure, the Practice must give notice by posting on the Practice's website for at least 90 days, or by placing a notice in a major print or broadcast media in the geographic area where the patients most likely reside.

10.2.3 If the Practice does not have current contact information on 500 or more patients affected by the unauthorized disclosure, the Practice must give notification through major media outlets serving the state in which the Practice is located.

10.2.4 The written notification given to patients will include, to the extent possible, the following:

- A brief description of what happened, including the date of the unauthorized disclosure and the date of its discovery;
- A description of the type of health information involved in the disclosure (e.g. name, Social Security number, date of birth, diagnoses, etc.);
- The steps the patient should take to protect himself/herself from potential harm resulting from the disclosure;
- A brief description of what the Practice is doing to investigate the disclosure, mitigate its impact and to protect against future unauthorized disclosures; and

- Contact information for the patient to ask questions (a toll free telephone number, email address, website or postal address). The template in Appendix I may be used to assist in preparing the notification to the patient.
- 10.2.5 The notice to patients described in subsection 10.2.4 must be provided as soon as possible, but in no event later than sixty (60) days after discovery of the unauthorized disclosure by the Practice.
- 10.2.6 If the unauthorized disclosure involved less than 500 patients, the Practice must maintain a log of the incident and submit the log to the federal Department of Health and Human Services (DHHS) at the end of the calendar year. If the disclosure involves more than 500 patients, the Practice must notify DHHS immediately.
- 10.3 **Exceptions.** Patient notification of an unauthorized disclosure of PHI will not be required where:
- 10.3.1 The disclosure is to a member of the Practice’s workforce, was made in good faith, and does not result in further disclosure;
- 10.3.2 The disclosure is made under circumstances in which it is unlikely that the unauthorized recipient would be able to retain the information.

Note: This is a new provision relating to situations where patient privacy and security has been breached. The form found in Appendix I is to be used where such breaches have occurred.

11. Technical Standards Published by the Federal Government Regarding Security of PHI

From time to time, the Department of Health and Human Services may publish guidance on technologies and methodologies that will render PHI unusable, unreadable or indecipherable to unauthorized individuals. The Security Officer will review this guidance, if any, on a quarterly basis, and determine whether such may be implemented in the Practice's electronic systems.

Note: This is a new provision and Practitioners are encouraged to use the HHS website for guidance on technical standards for security of ePHI.

12. Record Retention and Disposal

- 12.1 **Policies and Procedures Maintained.** The Practice will keep and maintain written policies and procedures that reflect its compliance with HIPAA Security Rule.
- 12.2 **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.
- 12.3 **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.

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.

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.
- 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.

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.

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 password 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.

2. Audit Controls

If practicable, 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.

3. Integrity of ePHI

The Practice will protect ePHI from improper alteration or destruction by means of the following:

- virus protection software
- computer firewall
- system back-ups
- electronic signatures

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.

5. Transmission Security

The Practice will guard against unauthorized access to ePHI transmitted over an electronic communications network. In particular, the Practice will not send patient health information in unencrypted e-mails over the Internet.