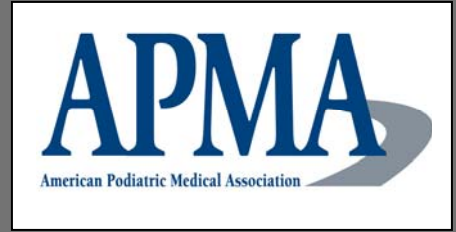


2010



HIPAA Privacy 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 Privacy 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 Privacy 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
About the Author	1
Who Must Comply With HIPAA?.....	1
Commonly Used Terms	2
HIPAA and Your State’s Law	3
POLICIES AND PROCEDURES	4
Section A: Workforce Policies	5
1. Personnel Designations.....	6
2. Training of Practice Personnel.....	7
3. Workforce Discipline.....	8
Section B: General Policies Regarding Disclosure of Patient Health Information9	
1. General Statement.....	10
2. Patient Authorization	11
3. Verification	12
4. Limiting Disclosures and Requests to the Minimum Necessary Information	14
5. Health Information of Deceased Patients	16
6. Disclosures for Workers’ Compensation Purposes.....	17
7. Sale of Patient Records	18
Section C: Disclosures Without Patient Authorization	19
1. General Statement.....	20
2. Disclosures to Parents and Other Authorized Representatives	21
3. Disclosures to Close Friends and Family Members	22
4. Disclosures Required by Law	23
5. Disclosures to Prevent Serious Threats to Health or Safety	27
6. Disclosures to Business Associates	28
7. Other Disclosures Which May Not Require Patient Authorization.....	29
Section D: Patient Rights.....	31
1. General Statement.....	32
2. Right to Notice.....	33
3. Right to Request Restrictions.....	34
4. Right to Confidential Communications	35
5. Right to Access	36
6. Right to Amend.....	38
7. Right to an Accounting	40
8. Waivers of Patient Rights and Non-Retaliation.....	42
Section E: Organizational Matters.....	43
1. Notice of Privacy Practices.....	44
2. Patient Complaints	45
3. Mitigation of Improper Disclosures.....	46

4.	Privacy and Security Safeguards	47
5.	Record Retention and Disposal.....	48
6.	Designated Record Set.....	49

APPENDIX A	Notice of Privacy Practices
APPENDIX B	Sample Business Associate Agreement
APPENDIX C	Patient Authorization to Release Health Information
APPENDIX D	Practice Resolutions
APPENDIX E	Privacy Training and Education Log
APPENDIX F	Patient Complaint Form
APPENDIX G	Accounting of Disclosures Forms
APPENDIX H	Glossary of Terms
APPENDIX I	HIPAA Resources
APPENDIX J	Request for Correction/Amendment of Health Information
APPENDIX K	Restriction Request Form
APPENDIX L	Request for Confidential Communications
APPENDIX M	Quick Reference Regarding Disclosures Requiring/Not Requiring Written Patient Authorization
APPENDIX N	Acknowledgment of Receipt/Review of HIPAA Privacy Manual

INTRODUCTION

About this Manual

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rules (Privacy Rules) took effect in 2003. At that time, the APMA commissioned the preparation of a HIPAA Privacy Manual for its members. The original Privacy Rules remained the same for nearly six years. 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 Privacy Rules and has necessitated the present revision to the APMA's 2003 Privacy Manual. This revised HIPAA Privacy Manual is intended to completely replace the prior version.

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.

Who Must Comply With HIPAA?

The Privacy Rules apply to, and must be followed by, those health care providers who conduct certain "standard electronic transactions." The following are the primary standard electronic transactions:

- Health care claims
- Eligibility determination for health plan coverage
- Referral certification or authorization
- Health care claim status
- Enrollment/disenrollment in a health plan
- Payment and remittance advice
- Health plan premium payments
- Coordination of benefits

If a health care provider conducts any of the above transactions, even just once, he or she must comply with the Privacy Rules, as set forth in this Manual. For example, most podiatric physicians today bill (i.e., submit health care claims) electronically. Because the submission of health care claims in electronic form is one of HIPAA’s “standard electronic transactions,” those who bill electronically must comply with the Privacy Rules. Likewise, many health care providers electronically check the eligibility of patients for health insurance benefits; some also receive EOB’s or remittance advice electronically. Such activities subject the provider to compliance with the Privacy Rules.

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)
Manual	This APMA HIPAA Privacy Manual
HIPAA	Health Insurance Portability and Accountability Act of 1996

HIPAA and Your State's Law

State privacy laws that do not conflict with the HIPAA Privacy Rules will remain in effect and are not superceded by the Privacy Rules. As to state laws that do conflict with the Privacy Rules, those laws will remain in effect if (1) they are more protective of privacy rights, or (2) it is possible to comply with both state law and the Privacy Rules. The HIPAA Privacy Rules take precedence over and supercede state laws that are less protective of patient privacy. In addition, HIPAA supercedes any state law that grants less access by patients to their own health information than does HIPAA. As a practical matter, few state laws will be preempted or superceded by HIPAA. Thus, in those instances where state laws exist, health care providers will generally continue to follow them.

For the reasons stated above, podiatrists should inform themselves as to their particular state's privacy laws, if any, and compare them to HIPAA's requirements. (For information about your state's privacy laws, see www.healthprivacy.org.)¹ To the extent that state law governs on a specific issue, the provisions of this Manual should be revised accordingly in consultation with legal counsel.

¹ This website may not be a final or complete source of state law.

POLICIES AND PROCEDURES

Section A: Workforce Policies

Section B: General Policies Regarding Disclosure of Patient Health Information

Section C: Disclosures Without Patient Authorization

Section D: Patient Rights

Section E: Organizational Matters

Section A: Workforce Policies

1. Personnel Designations

1.1 **Privacy Officer.** The Practice will designate a person to act as its privacy officer. The privacy officer will have responsibility for the overall implementation and oversight of the Practice's compliance with the HIPAA Privacy Rules. Specifically, the privacy 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 patient complaints pursuant to Section E.2, and take appropriate action in response.
- Receive and respond to patient requests under the Patient Rights provisions in Section D.
- Maintain all documentation required by this Manual and the HIPAA Privacy Rules.

1.2 **Contact Person.** The Practice will designate a "contact person," to whom patients may make inquiries or submit complaints regarding the Practice's privacy policies, procedures or conduct. The Practice may choose to have its privacy officer and contact person be the same person. The Practice's Notice of Privacy Practices will state the name of its privacy officer and contact person.

2. Training of Practice Personnel

- 2.1 **Training – Generally.** The Practice will train all Practice personnel regarding the HIPAA Privacy Rules, as well as this Manual, as necessary and appropriate for personnel to carry out their respective job duties.
- 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 thirty (30) 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 Privacy Rules or this Manual.
- 2.3 **Documentation of Training.** Training of Practice personnel will be recorded in the Privacy Training and Education Log (Appendix E), 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 privacy 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.
 - Review of this Manual.
 - Attendance at programs and seminars.
 - Review of professional literature and publications.
 - Use of Internet resources (Appendix I).
 - 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. Workforce Discipline

3.1 **Enforcement of Privacy Policies.** All Practice personnel are expected to adhere to the policies and procedures set forth in this Manual. Employees 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 Privacy Rules.
- Demotion or reassignment of job duties.
- Termination.

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

3.2 **Reporting of Privacy Violations.** Practice personnel are encouraged to report any violation of the provisions of this Manual to the privacy officer. The Practice will not retaliate against any employee for reporting a privacy violation or for supporting a patient's privacy rights.

3.3 **Prevention of Further Violations.** To the extent that privacy violations or deficiencies are reported or discovered, the Practice will take reasonable steps to ensure that similar violations do not occur in the future.

Section B: General Policies Regarding Disclosure of Patient Health Information

1. General Statement

The Practice will not use or disclose patient health information except as allowed by the HIPAA Privacy Rules, other federal and state laws, and the provisions of this Manual.

2. Patient Authorization

- 2.1 **General Statement.** Except in those situations described in Section C of this Manual, patient health information may not be disclosed unless a written authorization has been signed by the patient.
- 2.2 **Valid Authorizations.** To be a valid authorization, the authorization must:
- Be in writing;
 - Be signed and dated by the patient or his/her authorized representative;
 - Not have expired or been revoked;
 - Be filled out completely;
 - Contain language required by HIPAA; and
 - Not be combined with, or a part of, any other document.
- 2.3 **Form of Authorization.** Practice personnel shall ensure that patient authorizations are in a form the same as or similar to that found in Appendix C, or that the authorization have the same or similar content as Appendix C.
- 2.4 **Revocation of Authorization.** A patient may revoke his/her authorization at any time, so long as the revocation is in writing and signed by the patient.
- 2.5 **Copy to the Patient.** The patient must be given a copy of all authorizations he/she signs.

3. Verification

3.1 **General Statement.** Prior to disclosing patient health information, Practice personnel should verify the identity and authority (where applicable) of the person or entity requesting the information.

3.2 **Verification Protocols.** The following verification protocols will be followed by Practice personnel prior to making disclosures of patient health information:

3.2.1 As to patients:

3.2.1.1 If the patient appears in person and is known to Practice personnel, no verification is necessary; or

3.2.1.2 If the patient appears in person and is not known to Practice personnel, verification should be obtained by requesting photo identification, such as a driver's license; or

3.2.1.3 If a person purporting to be a patient calls the Practice, the identity of the person should be accomplished by asking simple identifying questions such as date of birth, Social Security number or mother's maiden name.

3.2.2 As to law enforcement or other public officials:

3.2.2.1 If the request is made in person, Practice personnel should request to see the officer's or official's identification badge or official credentials; or

3.2.2.2 If the request is made in writing, it is sufficient if it is on appropriate government letterhead; or

3.2.2.3 If the request is made by a person acting on behalf of a public official, Practice personnel should obtain a written statement on appropriate government letterhead showing the authority of the person making the request.

Patient health information will not be given by telephone to law enforcement or public officials except as provided in Section C.5.

3.2.3 As to health care providers who are treating the patient or insurance companies paying for treatment:

- 3.2.3.1 If the health care provider or insurance company is known to the Practice, no further verification is necessary; or
 - 3.2.3.2 If the health care provider or insurance company is not known to the Practice, a written request (by fax or mail) on their letterhead shall be requested for verification.
- 3.3 **Documentation.** To the extent that verification is required by subsection 3.2, such will be documented or noted in the patient's chart.

4. Limiting Disclosures and Requests to the Minimum Necessary Information

4.1 **General Rule.** The Practice will make reasonable efforts to limit its disclosures of, and requests for, patient health information to the minimum necessary information needed to accomplish the purpose of the disclosure or request. Except as allowed below, the Practice will not request or disclose the patient's entire medical record unless such is justified to accomplish the purpose of the request.

4.2 **Information Requests Received By the Practice.**

4.2.1 Whenever possible, the Practice will redact or delete the following items from the information disclosed to others:

- Names;
- Postal address information, other than town or city, state, and zip code;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images;

If the above items are not deleted, the Practice should document the reason for such.

4.2.2 For health information requests received by the Practice on a routine and reoccurring basis, the Practice will develop and follow protocols that limit the information disclosed to that which is reasonably necessary to achieve the purpose for the request;

4.2.3 For all other requests, the Practice will develop and follow criteria designed to limit the information disclosed to that which is reasonably

necessary to achieve the purpose of the request, and will review the request on an individual basis in accordance with that criteria.

4.3 **Requests Made By the Practice to Others for Information.**

4.3.1 For health information requests made by the Practice to others on a routine and reoccurring basis, the Practice will develop and follow standard protocols that limit the information requested to that which is reasonably necessary to achieve the purpose for the request;

4.3.2 For all other requests, the Practice will develop and follow criteria designed to limit the information requested to that which is reasonably necessary to achieve the purpose of the request, and will review the request on an individual basis in accordance with that criteria.

4.4 **Exceptions.** Practice personnel will not be required to follow the rules stated above in the following situations:

- Disclosures or requests to a health care provider for purposes of treatment.
- Disclosures to the patient.
- Disclosures or requests made pursuant to the patient's written authorization.
- Disclosures to Health and Human Services (HHS).
- Disclosures required by the HIPAA Privacy Rules.
- Disclosures required by law (see Section C.4).

4.5 **Minimum Necessary Workforce Access to Patient Health Information.**

Practice personnel who do not have a legitimate need to have access to patient health information to carry out their duties shall be restricted from having such access. The privacy officer will determine, in his/her discretion, whether access should be denied to any Practice personnel.

Note: Section 4.2 is a new provision. At times, the Practice may choose not to redact the items listed in section 4.2.1 and should simply document the reason for this.

5. Health Information of Deceased Patients

- 5.1 **General Statement.** Health information of deceased patients will be given the same protections as health information of living patients.
- 5.2 **Executors and Personal Representatives.** Legally authorized executors or personal representatives of deceased patients are entitled to act on behalf of the deceased patient with respect to the patient's health information. All patient rights and protections set forth in this Manual must be afforded to such executors or personal representatives.

6. Disclosures for Workers' Compensation Purposes

Disclosures of patient health information for purposes of workers' compensation benefits may be made pursuant to state workers' compensation laws and regulations.

7. Sale of Patient Records

The Practice will not sell patient records to a third party unless –

- The patient has consented in writing; or
- The Practice is being sold to another health care provider who is a covered entity under HIPAA regulations.

Section C: Disclosures Without Patient Authorization

1. General Statement

- 1.1 **Disclosures Allowed Without Patient Written Authorization.** In the following circumstances, the Practice may disclose patient health information without the patient's written authorization:
- 1.1.1 To the patient himself/herself, upon request.
 - 1.1.2 To other persons or entities for purposes of:
 - The Practice's treatment (as defined in Appendix H) of the patient.
 - Obtaining payment (as defined in Appendix H) for the Practice's services.
 - The Practice's "health care operations" (as defined in Appendix H).
 - 1.1.3 To another health care provider for the purpose of that provider's treatment of the patient.
 - 1.1.4 To other health care providers or HIPAA covered entities (as defined in Appendix H) for the purpose of their making or obtaining payment for health care services provided to the patient.
 - 1.1.5 To another HIPAA covered entity (as defined in Appendix H), but only if that entity either has or had a relationship with the patient whose health information is being requested, the information requested pertains to that relationship, and the information is for the purpose of the following "health care operations":
 - 1.1.5.1 Conducting quality assessment and improvement activities, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination; contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; or
 - 1.1.5.2 Reviewing the competence or qualifications of health care professionals; evaluating practitioner and provider performance, or health plan performance; conducting training programs in which students, trainees or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers; training of non-health care professionals; accreditation, certification, licensing or credentialing activities.

2. Disclosures to Parents and Other Authorized Representatives

- 2.1 **Guardians and Conservators.** If, under Idaho law, a person has legal authority to act for the patient as a guardian, conservator or holder of a power of attorney, the Practice may treat that person as if he/she is the patient as to all matters within the scope of that representative's authority. Practice personnel will request documentation (and keep a copy in the patient's file) from the representative to verify their authority to act on behalf of the patient.
- 2.2 **Parents of Unemancipated Minors.** If, under Idaho law, a parent or other person acting *in loco parentis* (a guardian or temporary custodian, foster parent, etc.) of an unemancipated minor has authority to act for the minor in making decisions related to health care, the Practice may treat that person as if he/she is the patient and will grant him/her the same rights and protections set forth in this Manual. As to guardians, foster parents or temporary custodians, Practice personnel will request documentation (and keep a copy in the patient's file) to verify their authority to act on behalf of the patient.
- 2.3 **Domestic Violence, Abuse or Neglect.** The Practice may decline to recognize a guardian, conservator, parent or other personal representative if, under Idaho law, the Practice has reason to believe that the patient has been or may be subjected to domestic violence, abuse or neglect by that person, or that recognizing such a person as the patient's representative could endanger the patient.
- 2.4 **Rights of Minors Under State Law.** If Idaho law allows an unemancipated minor to consent to obtain health care without parental consent, the Practice will not treat the parent as the minor's representative.

3. Disclosures to Close Friends and Family Members

- 3.1 **General Statement.** In the situations described below, Practice personnel may disclose patient health information to family members, relatives or close personal friends of the patient.
- 3.2 **Disclosures to Family Members or Closer Personal Friends.** Practice personnel may disclose to family members, relatives or close personal friends of the patient that health information directly relevant to such person's involvement in caring for the patient or paying for the patient's care if:
- The patient is physically present at the time of the disclosure and either agrees verbally or does not object to the disclosure, or Practice personnel reasonably infer from the circumstances that the patient does not object; or
 - The patient is not physically present or is incapacitated (unconscious, sedated, etc.) and Practice personnel determine that a disclosure of limited information would be in the patient's best interests. For example, Practice personnel may make limited disclosures to allow family, friends or relatives to pick up filled prescriptions, medical supplies, X-rays or similar items for the patient if Practice personnel determine that such would be in the patient's best interests.
- 3.3 **Other Disclosures to Caregivers.** Practice personnel may disclose patient health information to locate and notify a family member, personal representative or other person responsible for the patient's care of the patient's location, general condition or death if:
- The patient is physically present at the time of the disclosure and either agrees verbally or does not object to the disclosure, or Practice personnel reasonably infer from the circumstances that the patient does not object; or
 - The patient is not physically present, is incapacitated (unconscious, sedated, etc.) or deceased, and Practice personnel determine that a disclosure of limited information would be in the patient's best interests.

4. Disclosures Required by Law

- 4.1 **General Statement.** In certain circumstances, as described below, Practice personnel may disclose patient health information when required by law to do so. In such situations, the disclosure of patient health information should always be limited to only that which is required by law.
- 4.2 **Public Health Reporting.** Patient health information may be disclosed to:
- A public health authority that is authorized to receive information for the purpose of preventing or controlling disease, injury or disability (e.g., reporting of communicable diseases, births, deaths, etc.).
 - A public health authority or other appropriate government authority authorized to receive reports regarding suspected child abuse or neglect (as defined by state law).
 - Drug company representatives or medical device company representatives regulated by the FDA, for purposes of (1) reporting adverse events involving the drug or device; (2) tracking FDA related products; (3) enabling product recalls, repairs or replacements; or (4) conducting post marketing surveillance.
 - A person who may have been exposed to a communicable disease or who may be at risk of contracting a disease or condition, if state law authorizes the Practice to notify the person as part of a public health investigation or intervention.
- 4.3 **Victims of Abuse, Neglect or Domestic Violence.** Practice personnel may disclose patient health information regarding a patient believed to be the victim of abuse (other than child abuse), neglect or domestic violence to a government authority authorized by law to receive reports of such abuse, neglect or domestic violence where:
- The disclosure is required by state law;
 - The patient agrees to the disclosure; or
 - The disclosure is allowed by state law and Practice personnel believe the disclosure is necessary to prevent serious harm to the patient or other potential victims, or the patient is incapacitated and a law enforcement officer or authorized public official states that the information will not be used against the patient and that waiting for the information would adversely impact immediate enforcement activity.

If a disclosure of patient health information is made for the reasons described in this subsection 4.3, the patient must be informed that the disclosure has been or will be made unless informing the patient would put him/her at risk of serious harm. Practice personnel need not inform a parent, guardian, conservator or other personal representative of the disclosure if it is reasonably believed that such a person is responsible for the abuse, neglect and domestic violence, and that informing them would not be in the patient's best interests.

4.4 **Health Oversight Activities.** Practice personnel may disclose patient health information to federal or state agencies for purposes of :

- audits;
- civil, administrative or criminal investigations or proceedings;
- inspections; or
- licensure or disciplinary actions;

relating to oversight of the health care system, government benefit programs and regulation of government programs for which health information is necessary.

4.5 **Judicial and Administrative Proceedings.** Practice personnel may disclose patient health information in relation to a judicial or administrative proceeding —

4.5.1 When ordered to do so by a court or administrative tribunal; or

4.5.2 Upon receipt of a subpoena or discovery request if –

4.5.2.1 The Practice receives an appropriate protective order from the court or tribunal that prohibits the parties to the case from using or disclosing the information for any purpose other than the proceeding, and requires the return to the Practice or destruction of the health information at the end of the proceeding; or

4.5.2.2 The patient has been notified in writing of the request for his/her health information, and the notice gave the patient sufficient information about the proceeding in order to allow the patient to raise an objection to the court or tribunal by a certain date, and the patient has not objected to the disclosure within the specified time period, or the court/tribunal has resolved the patient's objections.

4.6 **Law Enforcement.**

4.6.1 Disclosures required by orders, warrants or subpoenas. Practice personnel may disclose patient health information to a law enforcement official for law enforcement purposes in the following situations:

- Where state law requires the reporting of certain types of wounds or injuries (e.g., gunshot wounds);
- Upon receipt of a court order or court-ordered warrant;
- Upon receipt of a subpoena or summons issued by a judicial officer;
- Upon receipt of a grand jury subpoena; or
- Upon receipt of an administrative subpoena, summons or investigative demand.

4.6.2 Identification of suspects, fugitives or witnesses. Other than in those situations described in subsection 4.6.1, above, Practice personnel may disclose only the following limited patient health information to law enforcement officials in response to their request made for purposes of identifying or locating a suspect, fugitive, material witness or missing person:

- Name and address
- Date and place of birth
- Social Security number
- ABO blood type and Rh factor
- Type of injury
- Date and time of treatment
- Date and time of death, if applicable
- A description of distinguishing physical characteristics

4.6.3 Patients who are crime victims. Practice personnel may disclose patient health information to a law enforcement official about a patient who is the victim of a crime if:

- The patient agrees to the disclosure; or
- The Practice is unable to obtain the patient's agreement due to his/her incapacity and the law enforcement official states that the information is needed to determine whether a crime was committed by someone other than the patient, immediate action depends upon the disclosure, and disclosure would be in the patient's best interests.

4.7 **Coroners and Funeral Directors.**

- 4.7.1 Practice personnel may disclose health information of a deceased patient to a coroner for the purpose of identifying a deceased person, determining the cause of death or other duties authorized by law.
- 4.7.2 Practice personnel may disclose health information of a deceased patient to a funeral director pursuant to applicable state law.

5. Disclosures to Prevent Serious Threats to Health or Safety

- 5.1 Unless otherwise prohibited by state law or professional ethical standards, Practice personnel may disclose patient health information if such disclosure —
- 5.1.1 Is necessary to prevent a serious and imminent threat to the health or safety of a person or the public, and is made to someone reasonably able to prevent the threat, including the target of the threat; or
- 5.1.2 Is necessary for law enforcement authorities to identify or apprehend the patient —
- 5.1.2.1 because of a statement by the patient admitting participation in a violent crime that caused serious physical harm to the victim; or
- 5.1.2.2 where it appears that the patient has escaped from a correctional institution or from law custody.
- 5.2 A disclosure made pursuant to subsection 5.1.2.1, above, must be limited to only the patient's statement and the following information:
- Name and address
 - Date and place of birth
 - Social Security number
 - ABO blood type and Rh factor
 - Type of injury
 - Date and time of treatment
 - Date and time of death, if applicable
 - A description of distinguishing physical characteristics

6. Disclosures to Business Associates

- 6.1 **Definition of Business Associates.** “Business associates” are third parties who provide services for the Practice and in so doing have access to patient health information. (Examples include: transcriptionists, billing services, clearinghouses, attorneys, accountants, collection agencies, etc.) Other treating health care providers are not business associates. (A more extensive definition may be found in Appendix H.)
- 6.2 **Requirement for Business Associate Agreements.** The Practice may disclose patient health information to its business associates if and only if the business associate has signed an agreement to protect patient privacy by following HIPAA Privacy Rules.
- 6.3 **Time for Obtaining Business Associate Agreements.**
- 6.3.1 If possible, the Practice shall have all of its current business associates sign an agreement the same as or similar to that found in Appendix B to this Manual prior to **<insert date>**.
- 6.3.2 Those business associates with whom the Practice forms a relationship after **<insert date>**, 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.
- 6.4 **Privacy Violations by Business Associates.** If the Practice or any of its personnel become aware that a business associate has violated or is violating its obligations under the business associate agreement, the Practice shall:
- Contact the business associate and request that such violations cease immediately; or
 - If the request to cease violations is not followed, terminate its relationship with the business associate.

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. Other Disclosures Which May Not Require Patient Authorization

7.1 **Research.** The practice may use or disclose patient health information for purposes of research projects provided that —

- The Practice obtains documentation that a waiver of patient authorization has been approved by either (1) an institution of review board (IRB) established pursuant to federal law, or (2) a privacy board composed of members with varying backgrounds and appropriate professional competency as necessary to review research protocols, and the board has at least one member who is not affiliated with the Practice or any entity conducting the research;
- The Practice obtains from the researcher a signed statement that patient health information is sought solely to prepare a research protocol or for similar purposes preparatory to research and that no health information will be removed from the Practice by the researcher in the course of his/her review; and
- The IRB or privacy board has determined that there is a minimal privacy risk to patients, there is an adequate plan to protect patient identifying information, and there is an adequate plan to destroy patient identifiers at the appropriate time consistent with the research.

7.2 **Marketing.**

7.2.1 **General statement.** “Marketing” means communications about a product or service that encourages someone to buy or use the product or service.

7.2.2 **Marketing activities that do not require authorization.** The Practice may engage in the following marketing activities (as defined in 7.2.1) without obtaining patient authorization:

- Communications to patients regarding their treatment;
- Communications regarding the case management or coordination of care of the patient;
- Recommendations to the patient regarding alternative treatments, therapies or health care providers; or

- Face-to-face discussions with the patient regarding health care products or services, so long as the Practice discloses any compensation it receives from the third parties to promote their products or services.

7.2.3 Other than those activities described in subsection 7.2.2, marketing activities require written patient authorization.

Section D: Patient Rights

1. General Statement

Practice personnel will recognize, uphold and enforce all patient rights established by the HIPAA Privacy Rules, and as set forth in this Section D of the Manual.

2. Right to Notice

All patients of the Practice have a right to receive a notice of the Practice's privacy policies and procedures. The Practice will prepare and post a notice of privacy practices. This notice will be provided to all patients on their first visit to the Practice after **<insert date>**. The notice will be posted in the Practice's lobby or reception area in a location accessible to all patients. If the Practice maintains a website, the notice of privacy practices will be posted on the website.

3. Right to Request Restrictions

- 3.1 **General Statement.** Patients have a right to request that the Practice restrict the uses or disclosures of patient health information to carry out treatment, payment or health care operations, and have a right to request that the Practice restrict disclosures made to family, relatives and close personal friends.
- 3.2 **Written Request.** Patients who request restrictions on the use or disclosure of their health information will be asked to fill out the Restriction Request Form as found in Appendix K.
- 3.3 **Procedure.** If the Practice receives a written request to restrict the uses and disclosures of patient health information, the request will be referred to the privacy officer for handling. The privacy officer will notify the patient in writing within a reasonable time as to whether the Practice will agree to the restriction. If the privacy officer advises the patient that it will not agree to the restriction, no further action is necessary. If the Practice advises the patient that it will abide by the restriction, a notation will be made prominently in the patient's chart, and the Practice will abide by that restriction from that date forward.
- 3.4 **Mandatory Restrictions.** The Practice must accept and honor a request for restriction from the patient if –
- 3.4.1 The potential disclosure would be to an insurance company for purposes of payment or health care operations; and
- 3.4.2 The protected health information pertains solely to a health care item or service for which the patient has paid out of pocket in full.
- 3.5 **Disclosures Required by Law.** The Practice will not agree to restrict disclosures of health information that are required by law.
- 3.6 **Termination of Restrictions.** If the Practice has agreed to a restriction on uses or disclosures of health information, it may terminate that agreement by advising the patient in writing that the termination will only be effective with respect to health information created or received after written notification to the patient. As to health information created or received prior to that date, the restriction must be followed.
- 3.7 **Documentation.** All patient requests for restrictions, along with the Practice's response thereto, shall be kept for a minimum of six (6) years from the date of the document(s).

Note: Section 3.4 is a new patient rights provision.

4. Right to Confidential Communications

- 4.1 **General Statement.** Patients have a right to request reasonable accommodations in receiving communications of their health information by alternative means or at alternative locations.
- 4.2 **Written Request.** Patients who request confidential communications will be asked to fill out the Request for Confidential Communications form, as found in Appendix L.
- 4.3 **Procedure.** Upon receipt of a request for confidential communications, the privacy officer will evaluate the request. If the request is reasonable, the privacy officer will note the request prominently in the patient's chart and adhere to the request. For example, if the patient requests that all communications be sent to an address different than the patient's home address, the Practice will adhere to that request and note it in the patient's chart. If the request is not reasonable, the privacy officer will notify the patient that the request has been rejected.
- 4.4 **Conditions to Providing Confidential Communications.** As a condition to providing confidential communications at the patient's request, the Practice may require that the patient provide assurances as to how payment for services will be provided.
- 4.5 **No Demand for Explanations.** The Practice may not require an explanation from patients as to the reason for requesting confidential communications.
- 4.6 **Documentation.** All patient requests for confidential communications, along with the Practice's response thereto, shall be kept for a minimum of six (6) years from the date of the document(s).

5. Right to Access

- 5.1 **General Statement.** Patients have a right to inspect and obtain a copy of their health information in the designated record set (as defined in Section E.6), except as noted herein.
- 5.2 **Procedure.** The practice may require that the patient request in writing to have access to his/her health information. Upon receipt of such a request, the Practice will provide the patient with an opportunity to inspect his or her health information within the following time frames:
- For records that are maintained on site, the Practice will provide access within 30 days from the receipt of the request from the patient;
 - For records not maintained on site, the Practice will provide access within 60 days of the date of receipt of the request from the patient.
- 5.2.1 The Practice will provide the patient with the health information in readable hard copy form. If the Practice maintains health information in electronic form, and the patient requests that the Practice transmit a copy in electronic form, the Practice will comply with this request. The Practice may provide the patient with a summary of the health information in lieu of providing access to the records themselves if and only if the patient agrees to receiving a summary and the patient agrees in advance to paying the fees imposed, if any, for the Practice providing the summary.
- 5.2.2 The Practice will provide a convenient time and place for the patient to inspect his/her health information or to obtain a copy of the information.
- 5.2.3 The Practice may charge a reasonable, cost-based fee for providing the patient with access to his/her health information. That fee may include copying charges, including the cost of supplies, and labor for copying, scanning or transmitting the information. The Practice may also charge postage if the patient has requested that the information be mailed. If the patient has agreed to a summary, the Practice may charge the costs of preparing the summary.
- 5.2.4 All requests by patients for access to health information will be referred to the privacy officer. In those circumstances in which access to health information is denied, the privacy officer will determine if some part of the patient's record may be disclosed without objection. If so, that portion of the record may be disclosed. As to all other parts of the record for which access is denied, the privacy officer will provide a timely, written denial to the patient stating the basis for the denial and, if applicable, the patient's right to have the denial reviewed. The written notice must also

explain to the patient that they may complain regarding the denial of access either to the Practice or to the Secretary of HHS. This notice will include the name, title and telephone number of the privacy officer.

- 5.2.5 All documentation regarding patient requests for access and any denials thereof, or any other documentation maintained under this subsection, must be retained by the Practice for a minimum of six (6) years from the date of the document(s).

5.3 **Denial of Access.**

- 5.3.1 Unreviewable grounds for denial. The Practice may deny patients access to health information that is created, maintained or is otherwise subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA) to the extent that providing access would be prohibited by that law, or where such information is made exempt under the CLIA law. In addition, a patient who is part of a research program may have his/her right of access temporarily suspended for as long as the research is in progress, provided that the patient has agreed to the denial of access at the time that he/she consented to participate in the research.

5.3.2 Reviewable grounds for denial of access.

- 5.3.2.1 The Practice may deny the patient access to his/her health information if the Practice reasonably believes that such access is likely to endanger the life or physical safety of the patient or another person, or that the information makes reference to another person and the Practice believes that allowing access may cause substantial harm to that person.

- 5.3.2.2 The Practice may deny access to a guardian, conservator or parent where the practice believes that such person is likely to cause substantial harm to the patient or another person by having access to the patient's health information.

- 5.3.2.3 If access to the patient's health information is denied for the above reasons, the patient has a right to have the denial reviewed by a licensed health care professional designated by the Practice as a reviewing official. This health care professional must be someone who did not participate in the original decision to deny access. The Practice will abide by the decision of that reviewing health care professional, to either grant or deny access to the patient.

6. Right to Amend

- 6.1 **General Statement.** Patients have a right to request that the Practice amend their health information in the designated record set (as defined in Section E.6).
- 6.2 **Procedure.** The Practice will follow the following procedures when a request to amend is received from a patient.
- 6.2.1 **Written request.** Patients who request amendments or corrections to their health information will be asked to fill out the Request for Correction/Amendment of Health Information form, as found in Appendix J. The requests will be referred to the privacy officer.
- 6.2.2 **Response to the patient's request.** After a reasonable investigation, the privacy officer will determine whether the practice will grant or deny the request to amend. The privacy officer will respond in writing to the patient's request within 60 days from the date of the request by either granting the amendment, or advising the patient of the denial of the request, as described below.
- 6.2.2.1 **Acceptance of amendment.** If the Practice accepts the patient's request for amendment, it will amend the patient's record and provide an appropriate link or reference to the location of the amendment. The Practice will also make reasonable efforts to provide the amendment within a reasonable time to those persons identified by the patient as having received health information about the patient and who need the amendment, and those persons, including business associates, who the Practice knows may have relied upon the information that is subject to the amendment.
- 6.2.2.2 **Denial of amendment.** If the Practice determines to deny an amendment, it must provide the patient with a timely, written denial stating the basis for the denial, the patient's right to submit a statement disagreeing with the denial and how the patient may file that statement. In addition, the Practice must inform the patient that he/she may request that the Practice provide a copy of the patient's request for amendment and the denial with any future disclosures of health information regarding the patient. The Practice must advise the patient that he/she is entitled to make a complaint and how such complaints may be submitted to the Practice or Secretary of HHS. This notice must include the name or title and telephone number of the Practice's privacy officer. If the patient, upon denial of the request to amend, submits a written statement disagreeing with

the denial, the Practice must include such statement with the patient's records and include that statement with any subsequent disclosure of the patient's health information to which the disagreement relates.

6.2.3 The Practice may deny a patient's request for amendment if the privacy officer determines that the health information subject to the request —

- was not created by the Practice;
- is not part of the patient's chart;
- would not be available for inspection under the provisions of this Manual; or
- is accurate and complete.

6.3 **Documentation.** All patient requests to amend their health information, along with the Practice's response thereto, shall be kept for a minimum of six (6) years from the date of the document(s).

7. Right to an Accounting

- 7.1 **General Statement.** Patients have a right to receive an accounting of disclosures of their health information made by the Practice and its business associates as set forth below.
- 7.2 **Procedure.** Patients requesting an accounting will be asked to make the request in writing. All requests for an accounting will be referred to the privacy officer. In responding to such requests, the privacy officer will follow the following procedures:
- 7.2.1 The privacy officer will respond to the patient's request no later than 60 days from the receipt of the request by providing the patient with a written accounting using the appropriate form in Appendix G (for electronic and non-electronic health information).
- 7.2.2 The Practice will retain a copy of all requests for accountings from patients as well as the accounting provided by the Practice to the patient for a minimum of six (6) years from the date of the document(s).
- 7.3 **Suspension of the Right to an Accounting.** The Practice may temporarily suspend the patient's right to receive an accounting of disclosures made to a health oversight agency or a law enforcement official for the time specified by that agency or official if giving the accounting would impede the agency's activities.
- 7.4 **Exceptions for Non-Electronic Health Records.** Patients shall have no right to an accounting as to disclosures of non-electronic health information —
- To carry out treatment, payment or health care operations (as defined in Appendix H);
 - To the patient;
 - Incident to a use or disclosure otherwise permitted by this Manual or the HIPAA Privacy Rules;
 - Pursuant to an authorization signed by the patient;
 - To correctional institutions or law enforcement officials; or
 - That occurred prior to April 14, 2003.
- 7.5 **Electronic Health Records.** If the Practice maintains health information in electronic form, the exceptions stated in subsection 7.4 do not apply.
- 7.5.1 The Practice is only required to give an accounting for disclosures of electronic health records which occurred within three (3) years of the patient's request.

- 7.5.2 The Practice must contact any Business Associates who have the patient's health information in electronic form and request that they provide the Practice with an accounting of all disclosures of the patient's electronic health information.
- 7.5.3 Alternatively, the Practice can provide an accounting of the disclosures it made and give the patient a list of all Business Associates (including contact information) who may possess the patient's health information in electronic form.
- 7.5.4 This section 7.5, and all subparts, applies only to disclosures of electronic health information that occur after January 1, 2011 [after January 1, 2014, for practices that had an EHR prior to January 1, 2009].

Note: Practitioners who use electronic health records should pay particular attention to new section 7.5.

8. Waivers of Patient Rights and Non-Retaliation

- 8.1 **No Waivers of Privacy Rights.** No patient or prospective patient will be asked to waive their rights under the HIPAA Privacy Rules as a condition to receiving health care services from the Practice.
- 8.2 **Non-Retaliation Policy.** Practice personnel will not intimidate or retaliate against patients who seek to inquire about, enforce or complain regarding their rights under the HIPAA Privacy Rules or this Manual.

Section E: Organizational Matters

1. Notice of Privacy Practices

- 1.1 **Preparation of the Notice.** The Practice will prepare a Notice of Privacy Practices the same or similar to that found in Appendix A. The Notice will contain those provisions required by the HIPAA Privacy Rules, and will be in two sections: a summary and an attached Notice of Privacy Practices (Notice). The entire Notice will be provided to patients.
- 1.2 **Providing the Notice to Patients.** The Practice will provide the Notice to each new patient who comes to the Practice after <insert date>; for existing patients, the Practice will provide the Notice at the time of the patient's first visit to the Practice after <insert date>.
- 1.3 **Posting the Notice.** The Notice will be posted or located prominently in the Practice's lobby or reception area. If the Practice has multiple offices or other locations where health care is provided, the Notice will be posted in each location. If the Practice has a website, the Notice will be posted on the website.
- 1.4 **Patient Acknowledgment.** Practice personnel will make a good faith effort to have each patient acknowledge in writing his/her receipt of the Notice at the time the Notice is provided pursuant to subsection 1.2, above. Acknowledgment may be accomplished by:
- The patient signing and dating a separate acknowledgment form;
 - The patient checking off a box on an intake form signed and dated by the patient; or
 - The patient initialing/signing and dating the Notice itself.
- Notation will be made as to patients who refuse to acknowledge receipt of the Notice.
- 1.5 **Document Retention.** The Practice will retain patient acknowledgments for a minimum of six (6) years from the date they are signed.

Note: The HITECH Act has required changes to the Notice of Privacy Practices. It is recommended that all patients receive a new copy of the amended notice (see Appendix A) on their first visit to the Practice following adoption of this manual.

2. Patient Complaints

2.1 **Notice to Patients.** The Practice will notify its patients, through the Notice of Privacy Practices, that they may make complaints regarding the Practice's policies, procedures and practices with respect to the HIPAA Privacy Rules. The Notice will also set forth the complaint process described below.

2.2 **Procedure for Patient Complaints.**

2.2.1 Patient complaints must be submitted in writing to the contact person designated by the Practice using the form in Appendix F.

2.2.2 Patient complaints will be reviewed by the privacy officer, and appropriate investigation, if any, will be conducted to develop the necessary information regarding the complaint.

2.2.3 Within fifteen (15) days of receiving the written complaint, the privacy officer will advise the patient, in writing, of the privacy officer's determination regarding the complaint, and the measures, if any, which will be taken by the Practice to mitigate any improper uses or disclosures of protected health information.

2.2.4 If the patient requests information to make a complaint to HHS, the privacy officer will provide the patient with HHS's address, as follows:

Office of Civil Rights
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Room 509F, HHH Building
Washington, D.C. 20201
(202) 619-0257
Email: ocrmail@hhs.gov

2.3 **Document Retention.** All documentation received or prepared in relation to a patient complaint will be kept a minimum of six (6) years.

2.4 **Non-Retaliation Policy.** Practice personnel will not retaliate against any patient who submits a complaint.

3. Mitigation of Improper Disclosures

If the Practice learns of an improper disclosure of patient health information, either through patient complaint or otherwise, the Practice will take immediate action to mitigate the impact of the disclosure to the extent possible. The Practice will also seek to mitigate, to the extent practicable, any improper disclosures of its business associates. For improper disclosures of patient health information, the Practice will follow the patient notification procedures set forth in Section B of the HIPAA Security Manual.

4. Privacy and Security Safeguards

The Practice will implement administrative, technical and physical safeguards to protect the privacy of patient health information as appropriate to the size, resources and circumstances of the Practice. These safeguards will be implemented as set forth in the Practice's HIPAA Security Manual. In particular, the Practice will take reasonable steps to prevent disclosures of patient health information in the following areas:

- reception and waiting room areas;
- hallways and treatment rooms;
- Patient record storage areas;
- fax machines and photocopiers;
- computer terminals and computer systems;
- portable electronic devices (laptops, PDA's, cell phones); and
- e-mail and other Internet communication.

5. Record Retention and Disposal

- 5.1 **Policies and Procedures Maintained.** The Practice will keep and maintain policies and procedures designed to ensure compliance with the HIPAA Privacy Rules.
- 5.2 **Document Retention Period.** The Practice will retain, for a minimum of six (6) years, all records, documents or information generated, created or required to be kept under the policies and procedures in this Manual, or as otherwise required by the HIPAA Privacy Rules.
- 5.3 **Storage in Secure Locations.** Records and information of the Practice will be kept or stored in safe, secure locations. Practice records stored offsite will be placed only in secure facilities.
- 5.4 **Disposal of Patient Health Information.** Patient health information (in whatever format or medium) will be disposed of using appropriate methods. Hard copy (paper) records will be disposed of by means of shredding, incineration or other methods that obliterate any identifying information in such records. Hard copy records or other health information will never be disposed of by placing such in a trash receptacle or dumpster.

6. Designated Record Set

6.1 **Matters Included in Designated Record Set.** The designated record set for patient health information shall include the following types of records or information:

- Patient medical files (whether in paper or electronic form);
- Patient financial, billing and collection information (whether in paper or electronic form); and
- Patient health information created or maintained by Business Associates;

to the extent that such is created or maintained for the purpose of making decisions about patients.

6.2 **Matters Not Included in Designated Record Set.** The following records, documents or information (whether in paper or electronic format) shall not be considered part of the designated record set:

- Quality improvement records;
- Risk management records;
- Psychotherapy notes;
- Cancer Registry information;
- Appointment or surgical schedules;
- Information compiled in anticipation of, or preparation for, civil, criminal or administrative proceedings;
- Patient health information exempt under the Clinical Laboratory Improvements Act (CLIA); or
- Other information exempt from disclosure under state or federal law.