

FCA HIPAA & SECTION 466.057, FLORIDA STATUTES, PRIVACY COMPLIANCE MANUAL

Prepared by:

Paul Watson Lambert, General Counsel
Florida Chiropractic Association, Inc.
30 Remington Road
Oakland, FL 34787
August 6, 2013

© Florida Chiropractic Association, Inc., 2013

Format Note

This document is in Word. Set the font at Times New Roman and the font size at 12 to have page numbers match the Table of Contents.

DISCLAIMER

This manual is designed to set forth the very minimum general policies and procedures that will satisfy the requirements of regulations implementing the HIPAA and HITECH Act called the Omnibus Rule. The manual is aimed at small to medium sized chiropractic practices. The manual is made available as a membership benefit at no cost for the exclusive use of doctors of chiropractic medicine who are members in good standing in the FCA. It is intended to be user friendly.

This manual may be too simple to satisfy the needs of some chiropractic practices. There are several excellent companies and individuals who have prepared very comprehensive manuals that may satisfy the needs of those practices that need more than this manual provides. FCA members are encouraged to check out and compare commercially available compliance manuals to determine whether one of those manuals serves that doctor's needs better than this manual. However, it is strongly recommended that any compliance manual considered, also, satisfy compliance with Section 456.057, Florida Statutes, and other applicable Florida Statutes.

There may be instances in which an FCA member sees a need to modify the manual to meet his particular practice situation. Any substantive modifications of the manual should be made in consultation with an attorney knowledgeable in the HIPAA regulations and Florida health law. The FCA assumes no responsibility for any modifications to the manual.

Please contact the FCA if any errors or incorrect information is found in the manual so that it may be corrected. FCA members are encouraged to periodically check the FCA web site and watch member e-bulletins for updates or corrections to the manual, and for articles, alert bulletins and answers to frequently asked questions. For further information or questions you may contact Paul Watson Lambert, FCA General Counsel, at 850 577-9028.

ACKNOWLEDGEMENTS

I acknowledge the help, education and graciousness of the members of the National Association of Chiropractic Attorneys who provided editing and comments on this manual and the following people who taught seminars on the HIPAA regulations at meetings of the National Chiropractic Attornes. I especially thank Marc Cohen, Esq., Ober, Kaler, Grimes & Shriver, 120 E. Baltimore St., Baltimore, MD 21202; Ross P. Lanzafame, Esq., Harter Secrest & Emery, 700

Midtown Tower, Rochester, NY 14604; and Howard Ross, 1100 W. Town & Country Road, Suite 1400, Orange, CA 92868. Marc, Ross and Howard spent many hours teaching the other members of the NACA about the ins and outs of the HIPAA regulations and made their compliance forms available for the rest of us to modify to comply with unique state law requirements and for use by members of the chiropractic associations represented by the NACA members.

TABLE OF CONTENTS

	Page
Instructions for using this manual	5
Steps to follow to comply with HIPAA	6 – 25

INDEX TO FORMS

Compliance Check List	26
Adoption of HIPAA Privacy Compliance Manual.....	27
Appointment of Privacy Officer and Contact Person.....	28
Notice of Privacy Practices.....	29 – 35
Acknowledgment of Receipt of Notice of Privacy Practices...	36
Patient’s Request for Copies of Records	37
Release of Patient Records Authorization	38
Accounting and Disclosures Form	39
Request for Correction or Amendment of Health Information	40
Patient Complaint Form	41
Request for Special Confidential Communications	42
Electronic Transfer or PHI Privacy Practice	43
Business Associate Agreement	44 – 49
Log of Business Associate Agreements	50
Privacy Training and Education Log	51
Notification to Patients and Media of Breach of PHI	52
Notification to Secretary of HHS of Breach of PHI	53

INSTRUCTIONS FOR USING THIS MANUAL

First, make sure that the print font for the manual is Times New Roman and font size is set at 12 to assure that the pages line up. This should be page 5. Follow all step-by-step instructions and fill in the blanks on each form before printing out the manual. Place the completed manual in a three ring binder notebook and keep the manual in a central place for easy reference. The term “practice” is used throughout the manual to mean the name of your practice. This manual complies with “Florida’s Mini-HIPAA Statute,” Section 456.057, Florida Statutes. HIPAA refers to the Health Insurance Portability and Patient Accountability Act of 1996. The HIPAA provides that it supersedes state laws relating to patient records privacy, except where the state law is stricter. There are several instances in which the provisions of Florida Statutes are stricter than the HIPAA regulations and supersede them. Those instances are taken into account in this manual. HITECH means the Health Information Technology for Economic and Clinical Act of 2009. Omnibus Rule refers to the rules adopted effective March 23, 2013.

The Omnibus Rule: *On Friday, January 25, 2013, the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) published the long-awaited final rule, entitled “Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules” (Omnibus Rule), 78 Fed. Reg. 5566 (Jan. 25, 2013). The Omnibus Rule is the combination of all rules relating to HIPAA and:*

- finalizes modifications to the Privacy, Security, and Enforcement Rules to implement the Health Information Technology for Economic and Clinical Health (HITECH) Act, proposed in July 2010;*
- finalizes modifications to the Privacy Rule, proposed in July 2010, to increase the workability of the Privacy Rule;*
- modifies the Breach Notification Rule, adopted by interim final rule in August 2009; and*
- finalizes modifications to the Privacy Rule to implement the Genetic Information Nondiscrimination Act of 2008 (GINA), proposed in October 2009.*

STEP ONE – READ THE INTRODUCTION CAREFULLY.

INTRODUCTION

OVERVIEW OF HIPAA REQUIREMENTS

HIPAA, HITECH and the Omnibus Rule require chiropractic physicians and other medical practices to maintain office policies and procedures that protect the confidentiality of patient health information. There are large fines, ranging from \$50,000 to \$1.5 million, attendant to breaches of that confidentiality and failure to maintain proof of adhering to policies and procedures protecting patient health information. The Office of Civil Rights in the U. S. Department of Health and Human Services is authorized to seek impositions of fines for violation of the HIPAA regulations and the Florida Attorney General is authorized to seek fines in the amount of \$5,000 for violations of Section 456.057, Florida Statutes.

WEB SITES WITH HELPFUL INFORMATION:

CMS HIPAA SITE:

<http://www.hhs.gov/ocr/privacy/>

The FCA offers this manual as one method of compliance with the Omnibus Rule and other regulations implementing the HIPAA/HITEC Omnibus Rule with an easy step-by-step process. Read through this overview then follow the step-by-step instructions.

WHAT IS HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes standards for the protection of patients' *protected health information* (PHI). The Omnibus Rule sets forth the procedures to protect PHI.

Following is a general discussion of the Omnibus Rule and compliance requirements for it.

The Omnibus Rule:

The Secretary of the U.S. Department of Health and Human Services (HHS) adopted regulations implementing HIPAA and HITECH. The regulations are known as the Omnibus Rule. The Omnibus Rule establishes national standards for the protection of certain health information and is the combination of the Privacy Rule and the Security Rule summarized below.

Compliance with the Omnibus Rule:

The Omnibus Rule requires providers to: (1) Develop notices informing patients of their privacy rights and provider practices regarding PHI ; (2) notify patients and the Secretary of HHS of a breach of PHI under certain circumstances; (3) prepare authorization forms for release of PHI; (4) draft and implement policies to protect patient medical records and provide patient access to those records; (4) bring business associate agreements into compliance with the new rules and (5) certify the practice and staff have been trained in Omnibus Rule standards and the practice's privacy practices.

The Security Rule:

In 2003 the Secretary of the HHS adopted the *Security Standards for the Protection of Electronic Protected Health Information* (the Security Rule) that establishes a national set of security standards for protecting health information that is held or transferred in electronic form. The Security Rule puts into operation the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that health care practices must implement to secure patient health information transmitted electronically or digitally. This is referred to as "electronic protected health information" (e-PHI). Within HHS, the Office for Civil Rights (OCR) has responsibility for enforcing the Privacy and Security Rules with voluntary compliance activities and civil money penalties. The Omnibus Rule completes the Privacy Rule and the Security Rule.

General Compliance with the Omnibus Rule

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI (electronic patient health information). Specifically, covered entities must:

Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;

Identify and protect against reasonably anticipated threats to the security or integrity of the information;
Protect against reasonably anticipated, impermissible uses or disclosures; and
Ensure compliance by their workforce.

The Security Rule defines “confidentiality” to mean that e-PHI is not available or disclosed to unauthorized persons. The Security Rule promotes the two additional goals of maintaining the integrity and availability of e-PHI. Under the Security Rule, “integrity” means that e-PHI is not altered or destroyed in an unauthorized manner. “Availability” means that e-PHI is accessible and usable on demand by an authorized person. HHS recognizes that *covered entities* (health care practices or businesses that electronically transmit PHI) range from the smallest provider to the largest, multi-state health plan. Therefore the Security Rule is flexible and scalable to allow covered entities to analyze their own needs and implement solutions appropriate for their specific environments. What is appropriate for a particular covered entity will depend on the nature of the covered entity’s business, as well as the covered entity’s size and resources. Therefore, when a covered entity is deciding which security measures to use, the Rule does not dictate those measures but requires the covered entity to consider:

Its size, complexity, and capabilities,
Its technical, hardware, and software infrastructure,
The costs of security measures, and
The likelihood and possible impact of potential risks to e-PHI.

Covered entities must review and modify their security measures to continue protecting e-PHI in a changing environment.

Security Rule Technical Safeguards

Access Control. A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).

Audit Controls. A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.

Integrity Controls. A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.

Transmission Security. A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

Physical Safeguards

Facility Access and Control. A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed.

Workstation and Device Security. A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI).

Access Control. A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).

Audit Controls. A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.

Integrity Controls. A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.

Transmission Security. A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

The HITECH Regulations:

Congress enacted the Health Information Technology for Economic and Clinical (HITECH) Act of 2009, as part of the American Recovery and Reinvestment Act. The HITECH Act requires the Office of Civil Rights to adopt regulations implementing the Act.

HHS issued regulations requiring health care providers, health plans, and other entities covered by the Health Insurance Portability and Accountability Act (HIPAA) to notify individuals when their health information is breached.

These “breach notification” regulations implement provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA).

The regulations require health care providers and other HIPAA covered entities to promptly notify affected individuals of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.

Breaches under the Omnibus Rule: The Omnibus Rule now raises a “rebuttable presumption” that a breach of PHI must be reported to patients whose PHI is compromised and the Secretary of the HHS. The presumption of a breach of confidentiality of PHI is rebutted if all four of the following points are met giving rise to “low probability of PHI compromise.”

1. The nature and extent of the PHI involved – issues to be considered include the sensitivity of the information from a financial or clinical perspective and the likelihood the information can be re-identified;
2. The person who obtained the unauthorized access and whether that person has an independent obligation to protect the confidentiality of the information;
3. Whether the PHI was actually acquired or accessed, determined after conducting a forensic analysis; and
4. The extent to which the risk has been mitigated, such as by obtaining a signed confidentiality agreement from the recipient.

Privacy and Security Policies and Procedures

The Omnibus Rule require changes to a physician practice’s HIPAA policies and procedures in at least the following areas:

Marketing communications: The new rules further limit the circumstances when physicians may provide marketing communications to their patients in the absence of the patient’s written authorization. Generally speaking, the only time a physician may tell a patient about a third-party’s product or service without the patient’s written authorization is when: 1) the physician receives no compensation for the communication; 2) the communication is face-to-face; 3) the communication involves a drug or biologic the patient is currently being prescribed and the payment is limited to reasonable reimbursement of the costs of the communication (no profit); 4) the communication involves general health promotion, rather than the promotion of a specific product or service; or 5) the communication involves government or government-sponsored programs. Physicians are also still permitted to give patients promotional gifts of nominal value (e.g., pamphlet).

Breach Notification: The Omnibus Rule raises a “rebuttable presumption” that a breach of PHI must be reported to patients whose PHI is compromised and the Secretary of the HHS. The presumption of a breach of confidentiality of PHI is rebutted if all four of the following points are met giving rise to “low probability of PHI compromise.”

1. The nature and extent of the PHI involved – issues to be considered include the sensitivity of the information from a financial or clinical perspective and the likelihood the information can be re-identified;
2. The person who obtained the unauthorized access and whether that person has an independent obligation to protect the confidentiality of the information;
3. Whether the PHI was actually acquired or accessed, determined after conducting a forensic analysis; and
4. The extent to which the risk has been mitigated, such as by obtaining a signed confidentiality agreement from the recipient.

Childhood immunizations: Under the Omnibus Rule, physicians may disclose immunizations to schools required to obtain proof of immunization prior to admitting the student so long as the physicians have and document the patient or patient’s legal representative’s “informal agreement” to the disclosure.

Deceased Patients: The Omnibus Rule allows physicians to make relevant disclosures to the deceased’s family and friends under essentially the same circumstances such disclosures were permitted when the patient was alive; that is, when these individuals were involved in providing care or payment for care and the physician is unaware of any expressed preference to the contrary. The new rule also eliminates any HIPAA protection for PHI 50 years after a patient’s death.

Copies of e-PHI: Physicians will now have only 30 days to respond to a patient’s written request for his or her PHI with one 30-day extension, regardless of where the records are kept (eliminating the longer 60-day timeframe for records maintained offsite). They must provide access to EHR and other electronic records in the electronic form and format requested by the individual if the records are “readily reproducible” in that format. Otherwise, they must provide the records in another mutually agreeable electronic format. Hard copies are permitted only when the individual rejects all readily reproducible e-formats. Florida Statute 456.057 requires that copies of a patient’s records be furnished within a reasonable time that may be interpreted to mean fewer than 30 days.

Emailing PHI: Physicians must also consider transmission security, and may send PHI in unencrypted emails only if the requesting individual is advised of the risk and still requests that form of transmission.

Charging for copies of e-PHI or PHI: Patients may now request copies of their records in electronic format under the 2013 regulations. Doctors should be prepared to furnish records on a compact disk (CD) or flash drive or by secure email. Records in paper format may be scanned and furnished to a patient. The Omnibus Rule allows charging a patient for the labor costs of providing the electronic records including the costs of the flash drive or CD unless state sets a lower fee. Current Florida statutes or Rules of the Board of Chiropractic Medicine do not address the authority of charging patients for a cost of furnishing patients records in an electronic or digital format. It is not known of the costs for charging for paper records will be applied to electronic records. • Research authorizations – The new rules permit physicians to combine conditioned and unconditioned authorizations for research participation, provided individuals can opt-in to the unconditioned research activity. Moreover, these authorizations may encompass future research.

Business Associate Agreements (BAA): Each health care practice is required to enter into a Business Associate Agreement or “BAA” (found at pages 44-49) with any other person or company that has access to protected patient information (PHI). Examples of business associates include third party administrators or pharmacy benefit managers for health plans, claims processing or billing companies, transcription companies, and persons who perform legal, actuarial, accounting, management, or administrative services for covered entities and who require access to protected health information. The HIPAA Rules define “protected health information” as the individually identifiable health information held or transmitted in any form or medium by these HIPAA covered entities and business associates, subject to certain limited exceptions. A BAA must be entered into with any Health Information Exchange Organization or Regional Health Information Organization as they are developed.¹

The Act requires HIPAA covered entities to provide notification to affected individuals and to the Secretary of HHS following the discovery of a breach of unsecured protected health information.²

Section 13400(1) of the Act defines “breach” to mean, generally, the unauthorized acquisition, access, use, or disclosure of protected health information that compromises the security or privacy of such information.

¹ See those entities described in section [164.502](#)(e)(2) of title 45, Code of Federal Regulations and a written contract (or other arrangement) described in section [164.308](#)(b) of such title, with such entity and shall be treated as a business associate of the covered entity for purposes of the provisions of this subtitle and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of the date of enactment of this title.

² Sections 164.502, et, *Seq.*, Title 45, Code of Federal Regulations implement the Act.

Section 13402(h) of the HiTech Act defines “unsecured protected health information” as “protected health information that is not secured through the use of a technology or methodology.

Section 13402(b) of the Act requires a business associate of a covered entity that accesses, maintains, retains, modifies, records, destroys, or otherwise holds, uses, or discloses unsecured protected health information to notify the covered entity when it discovers a breach of such information, so that the covered entity can notify affected patients.

Civil and Criminal Penalties

The HITECH Act introduced significant increases in civil and criminal penalties, which now apply not only to covered entities but also, for the first time, to business associates that have violated their HIPAA requirements. Depending on the violation, the Omnibus Rule sets the civil penalties range from \$50,000, up to a total of \$1.5 million per calendar year. The HITECH Act also provides the Department of Justice with broader and more explicit authority to prosecute and pursue criminal penalties for violations of this nature. If the Department of Justice decides not to act on a violation, the OCR may pursue civil penalties for the same violations. In addition, state Attorneys General now have clear authority to take enforcement action if citizens believe their medical privacy has been violated. This means that business associates are now subject to penalties in an environment that is open to more aggressive enforcement of the HIPAA Rules.

The Act and the Omnibus Rule require HIPAA covered entities to notify affected individuals and to the Secretary of HHS following the discovery of a breach of unsecured protected health information, unless there is a “low probability of PHI compromise.” In addition, in some cases, the Act requires covered entities to provide notification to the media of breaches. In the case of a breach of unsecured protected health information at or by a business associate of a covered entity, the Act requires the business associate to notify the affected patients, the Secretary of HHS and the media of the breach. The Omnibus Rule imposes responsibility on the business associate to assure any subcontractors are compliant with the Omnibus Rule and is responsible for breaches of PHI by the subcontractors. Finally, the Act requires the Secretary to post on an HHS Web site a list of covered entities that experience breaches of unsecured protected health information involving more than 500 individuals.

Protected health information (PHI) is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:

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

Definition of “encryption.” NIST Roadmap plans include the development of security guidelines for enterprise-level storage devices, and such guidelines will be considered in updates to this guidance, when available. Information on computer security is available at <http://www.csrc.nist.gov/>.

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

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

(b) The media on which the PHI is stored or recorded have been destroyed in one of the following ways:

(i) Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

(ii) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800–88, *Guidelines for Media Sanitization*, such that the PHI cannot be retrieved.

Actions to Take in a Breach of Patient Protected Health Information:

Section 13402 of the Act and the Omnibus Rule require covered entities and business associates to provide notification following a breach of unsecured protected health information. Section 13400(1)(A) of the Act defines “breach” as the “unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of the protected health information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.”

Section 13402(h) of the HiTech Act defines “unsecured protected health information” as “protected health information that is not secured through the use of a technology or methodology.

Section 13402(b) of the Act requires a business associate of a covered entity that accesses, maintains, retains, modifies, records, destroys, or otherwise holds, uses, or discloses unsecured protected health information to notify the covered entity when it discovers a breach of such information, so that the covered entity can notify affected patients.

Actions to Take Upon a Breach of PHI:

The Omnibus Rule raises a “rebuttable presumption” that a breach of PHI must be reported to patients whose PHI is compromised and the Secretary of the HHS. The presumption of a breach of confidentiality of PHI is rebutted if all four of the following points are met giving rise to “low probability of PHI compromise.”

1. The nature and extent of the PHI involved – issues to be considered include the sensitivity of the information from a financial or clinical perspective and the likelihood the information can be re-identified;
2. The person who obtained the unauthorized access and whether that person has an independent obligation to protect the confidentiality of the information;
3. Whether the PHI was actually acquired or accessed, determined after conducting a forensic analysis; and
4. The extent to which the risk has been mitigated, such as by obtaining a signed confidentiality agreement from the recipient.

In the event that it is determined that there is a high probability of PHI compromise, then the following steps are to be followed:

- Notice to patients of breaches “without reasonable delay” within 60 days of the breach following steps on the notification form found at page 51
- Notice to prominent media outlets when breaches affect more than 500 individuals
- Notice to next of kin when breaches affect deceased patients
- Notice to the HHS secretary of breaches without reasonable delay

Business Associate Agreements

Chiropractic physicians are “covered entities” under the Health Insurance Portability and Accountability Act, known as HIPAA. The U.S. Department of Health and Human Services issued the Omnibus Rule requiring health care providers to notify patients when their health information confidentiality is breached.

These “breach notification” regulations implement provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA).

The Omnibus Rule is effective as of March 23, 2013, as they apply to health care providers.

A Business Associate is someone who is not an employee of the Practice who has access to PHI. A Business Associate Agreement (BAA) is an agreement by which a Business Associate agrees to keep confidential any PHI to which the Business Associate is exposed.

Examples of business associates include third party administrators or benefit managers for health plans, claims processing or billing companies, transcription companies, and persons who perform computer maintenance, legal, actuarial, accounting, management, or administrative services for covered entities and who require access to protected health information. Business associates include lawyers who have any access to protected patient information. Many lawyers erroneously conclude that the confidentiality requirements attendant to a lawyer client relationship preempts the need for executing a business associate agreement. This is incorrect. A doctor, who does not obtain a properly executed business associate agreement from a lawyer or any vendor or person accessing protected patient information, does so at his or her own liability risk.

The breach notification regulations apply whenever patient protected information is revealed to someone who should not have access to it.³ The breach notification requirements apply whenever a “business associate” breaches the confidentiality of patient protected information.

Employees of or physicians in a practice are not business associates. They are required to maintain confidentiality of patient protected information by HIPAA and Florida Statutes.

Chiropractic physicians are required to enter into Business Associate Agreements with persons who are not employees of the practice who have access to “protected patient information.” Protected patient information, generally, includes any information about patients.

Unauthorized persons must protect any electronic transmission of protected patient information from access. That means that patient protected information transmitted by fax, email or other Internet methods should be encrypted. Computers on which protected information is stored must be secured. Business associates must agree to maintain the security of patient information stored on their computers and agree to transmit it in a secure manner.

STEP TWO - ADOPTION OF MANUAL: Adopt the FCA HIPAA Privacy Compliance Manual as your own by filling in the Practice Resolution Adoption of HIPAA Privacy Compliance Manual at Page 27.

³ The HIPAA Rules define “protected health information” as the individually identifiable health information held or transmitted in any form or medium by these HIPAA covered entities and business associates, subject to certain limited exceptions. The Act requires HIPAA covered entities (meaning chiropractic physicians) notify affected individuals and to the Secretary of HHS following the discovery of a breach of unsecured protected health information. Sections 164.502, ET, implement the Act. *Seq.*, Title 45, Code of Federal Regulations.

STEP THREE - DESIGNATION OF PRIVACY OFFICER / CONTACT PERSON:

Designate someone in the office, such as the office manager, as the “Privacy Officer” and “Contact Person.” A “Privacy Officer” is the individual in your practice responsible for seeing that the privacy procedures are adopted and followed: The privacy officer is designated by completion of the Appointment of Privacy Officer form at page 28 in the manual. The Privacy Officer will have responsibility for the overall implementation and oversight of the Practice’s compliance with the HIPAA Privacy Rules. Duties of the Privacy Officer are:

- Oversee the implementation of the privacy and protection policies and procedures.
- Ensure that all Practice personnel are trained regarding the privacy protection policies and procedures as appropriate for their positions and job functions.
- Provide a copy of the Notice of Privacy Practices to personnel and ensure that such personnel follow the policies and procedures contained herein.
- Investigate and respond to patient complaints relating to breach of privacy and take appropriate action in response.
- Receive and respond to patient requests under the Patient Rights provisions stated in the Notice of Privacy Practices.
- Maintain all documentation required by the Notices of Privacy Practices and the Omnibus Rule.

The “Contact Person” is the person to whom patients may make inquiries or submit complaints regarding the Practice’s privacy policies, procedures or conduct. The privacy officer and contact person may be the same person. The clinic’s Notice of Privacy Practices will state the name of its privacy officer and contact person.

STEP FOUR - NOTICE OF PRIVACY PRACTICES: Fill in the blanks of the Notice of Privacy Practices form found at pages 29-35. Print out a copy of the completed Notice of Privacy Practices and post a copy in a prominent place in the Practice’s patient waiting room and the Practice’s web site. **Posting of the Notice of Privacy Practices is required by the HIPAA regulations to be posted in a prominent place in the patient waiting room and on any web site of the Practice.** Existing patients are to be given a copy of the Notice of Privacy together with the Acknowledgement of Receipt of Notices of Privacy Practices (found at pages 29-35). Ask the patient to sign the Acknowledgment of Receipt of Notices of Privacy Practices and place the signed form in the patient’s file. Each new patient coming for examination or treatment is given a copy of the Notice of Privacy together with the Acknowledgement of Receipt of Notices of Privacy Practices on the initial patient visit. Place the new patient’s signed Acknowledgment of Receipt of Notices of Privacy Practices form in the patient’s file.

STEP FIVE - RELEASE OF PATIENT RECORDS TO PATIENT - OR, PATIENT WANTS RECORDS, PATIENT GETS RECORDS:

The HIPAA regulations require practices to release patient records and x-rays to patients upon their written request. Whereas, it is a good business practice to have a signed, written request from the patient to maintain in the patient's records, Florida Statutes do not require patients to sign or furnish written requests for their records. This is an example of Florida's laws superseding the HIPAA regulations because the Florida law is stricter than the HIPAA regulations.

A NOTE ON RETENTION, STORAGE AND DISPOSAL OF PATIENT RECORDS:

HIPAA requires records to be kept for six years preempting Florida Statute 460.313 (1)(m) and Board of Chiropractic Medicine Rule 64B2-17.0065 requiring chiropractic physicians to maintain patient records two years and x-ray for at least four years. Therefore, it is recommended that all patient records be maintained for at least six years to avoid any conflict with the HIPAA regulations. Patient files should be kept or stored in safe, secure locations. Records stored off site will be placed only in secure facilities. Documents containing Protected Health Information will be disposed of using appropriate methods such as by shredding. Computer discs should be destroyed to prevent retrieval of protected patient information, even if it is "erased." There are software programs that restore many erased data. There are software programs, such as used by the Department of Defense, that securely erase data. But, the safest method of destroying digital data is by destroying the disk or flash drive on which it is stored. Paper copies of patient records should never be placed in dumpsters, but securely shredded.

Florida Statute 456.057 (6) provides that any health care practitioner licensed by the Department of Health, Division of Medical Quality Assurance, which includes chiropractic physicians, who makes a physical or mental examination of, or administers treatment or dispenses legend drugs to, any person shall, upon request of such person or the person's legal representative, furnish, in a timely manner, without delays for legal review, copies of all reports and records relating to such examination or treatment, including X rays and insurance information. Section 456.057 (6) makes clear that the furnishing of such report or copies shall not be conditioned upon payment of a fee for services rendered.

Stated simply, if a patient orally or in writing asks for his or her records, patient is entitled to receive them in a timely manner even if the patient owes the doctor or practice money. A patient does not have to give a reason for the request for records.

As a practical matter, most patients will sign a request for records. Fill in the name of the Practice on the Patient's Request for Copies of Records form found at page 37. Have the form available to give to patients upon delivery of records to them. Make a note on the form that the patient was furnished the records but refused to sign the form, in the event that the patient does not want to sign the form. Keep a copy of the signed or unsigned form in the patient's file.

Section 457.057 (18), Florida Statutes, authorizes a health care practitioner or patient records owner furnishing copies of reports or records or making the reports or records available for digital scanning pursuant to this section to charge no more than the actual cost of copying, including reasonable staff time, or the amount specified in administrative rule by the appropriate board, or the department when there is no board. Patients get upset when they are charged for their records. A physician should weigh the effort of copying a patient's records upon request against the effects on the patient by charging for those copies.

Charges for Furnishing Records - Rule of the Board of Chiropractic Medicine:

64B2-17.0055 Release of Medical Records; Reasonable Costs of Reproduction.

(1) Any person licensed pursuant to Chapter 460, Florida Statutes, is required to release copies of patient medical records upon request of the patient or his legal representative.

(2) For patients and governmental entities, the reasonable costs of reproducing copies of written or typed documents or reports shall not be more than the following:

(a) For the first 25 pages, the cost shall be \$1.00 per page.

(b) For each page in excess of 25 pages, the cost shall be 25 cents.

(3) For other entities, the reasonable costs of reproducing copies of written or typed documents or reports shall not be more than \$1.00 per page.

(4) Reasonable costs of reproducing x-rays, and such other special kinds of records shall be the actual costs. The phrase "actual costs" means the cost of the material and supplies used to duplicate the record, as well as the labor costs and overhead costs associated with such duplication.

Rulemaking Authority 460.405 FS. Law Implemented 456.057(4), (16) FS. History--New 7-15-91, Amended 5-19-93, Formerly 21D-17.0055, 61F2-17.0055, 59N-17.0055, Amended 3-11-10.

The Omnibus Rule allows for a reasonable charge for providing digital records.

STEP SIX - RELEASE OF PATIENT INFORMATION TO ANY PERSON OTHER THAN PATIENT:

Florida Statute 456.057 (11) requires all records owners shall develop and implement policies, standards, and procedures to protect the confidentiality and security of the medical record. Employees of records owners shall be trained in these policies, standards, and procedures.

Fill in the name of the Practice in the Patient Authorization for the Use and Disclosure of Protected Health Information form found at page 38. Use this form whenever the Practice is asked to furnish a patient's records to any person other than the patient's legal representative. Florida Statute 456.057 is stricter than the HIPAA regulations regarding release of patient information and supersedes the HIPAA regulations. Florida Statute 456.057 prohibits furnishing to or discussion about information about the medical condition of a patient with ANY person other than the patient's legal representative or other health care practitioners and providers involved in the care or treatment of the patient except upon written authorization of the patient.

Florida Statute 456.057⁴ lists seven exceptions to this requirement. Under those seven exceptions, a practice may release patient records without patient authorization:

1. To an employer/carrier requesting the records for processing a Workers' Compensation claim;
2. To any person, firm, or corporation that has procured or furnished such examination or treatment with the patient's consent;
3. When compulsory physical examination is made pursuant to a judge's order, in which case copies of the medical records shall be furnished to both the defendant and the plaintiff;
4. In any civil or criminal action, unless otherwise prohibited by law, upon the issuance of a subpoena from a court of competent jurisdiction and proper notice to the patient or the patient's legal representative by the party seeking such records.
5. For statistical and scientific research, provided the information is abstracted in such a way as to protect the identity of the patient or provided written permission is received from the patient or the patient's legal representative;
6. In response to a valid subpoena issued by the Department of Health; or

⁴ See Florida Statute 456.057 (7)(a).

7. In a medical negligence action or administrative proceeding when a health care practitioner or provider is or reasonably expects to be named as a defendant, information disclosed to a health care practitioner by a patient in the course of the care and treatment of such patient is confidential and may be disclosed only to other health care practitioners and providers involved in the care or treatment of the patient, or if permitted by written authorization from the patient or compelled by subpoena at a deposition, evidentiary hearing, or trial for which proper notice has been given.

Florida Statute 456.057 makes clear that absent a specific written release or authorization permitting utilization of patient information for solicitation or marketing the sale of goods or services, any use of that information for those purposes is prohibited.

The HIPAA regulations require that a copy of the signed written authorization form be given to the patient and the release of PHI logged in the patient's file.

Florida Statute 456.057 (12) makes clear that any third party to whom records are disclosed is prohibited from further disclosing any information in the medical record without the express written consent of the patient or the patient's legal representatives. This prohibition applies to any person to whom patient records have been given with or without specific patient authorization.

STEP SEVEN - MAINTAINING A RECORD OF DISCLOSURES TO THIRD PARTIES:

The HIPAA regulations require practices to maintain a record of disclosures of their patient information with some exceptions. The HIPAA regulations give patients a right to an accounting from the Practice of the names and dates of those disclosures. However, Florida Statute 456.057 (10) has a stronger provision that has no exceptions. So, the details of the HIPAA regulation are not discussed in lieu of discussion of the Florida Statute.

Florida Statute 456.057 (10) provides that records owners are responsible for maintaining a record of all disclosures of information contained in the medical record to a third party, including the purpose of the disclosure request. It is the responsibility of the Privacy Officer to log all patient information disclosures. A form for accounting of all disclosures is found at page 39. The record of disclosure may be maintained in the medical record. The record of disclosure becomes part of the medical records, if the record of disclosure is maintained as part of the medical record. Therefore, as discussed above, a patient is entitled to a copy of his or her medical records by simply asking for them. Such a request would include the disclosure recordations. It is recommended that all recordations of disclosures of medical records be maintained on the form found on page 39 and maintained in the respective patient medial records for simplicity of records keeping.

The HIPAA regulations require requests for an accounting of disclosures to be in writing. However, as discussed above, Florida Statute does not require a request for an accounting of disclosures to be in writing if the record of disclosure is maintained as part of the patient's records. Never the less, there is at page 39 a form requesting an accounting of disclosures to submit to patients requesting such an accounting.

STEP EIGHT - PATIENTS' RIGHT TO AMEND RECORDS:

The HIPAA regulations give patients the right to request that their patient information found in their medical records be amended. The request to amend must be in writing. A patient requesting amendment of their patient information should be given a request form found at page 40. The name of the Practice should be inserted now in the appropriate space in the form. Usually, a request for amendment of patient information comes after a patient has reviewed his or her medical file. The request to amend should be given to the Privacy Officer for processing. The Privacy Officer will respond in writing to the patient within 60 days from the date of the request and advise the patient as to whether the request is granted or denied. The Privacy Officer will make reasonable efforts to provide the amendment, if it is done, to those persons identified by the patient as having received information about the patient and who need the amendment. The Privacy Officer will, also, notify those persons, including business associates, who are known to have relied upon the unamended information.

Errors in a medical record brought to the Practice's attention by a patient are candidates for amendments. However, Board of Chiropractic Medicine Rule 64B2-17.0065 set forth the requirement for maintaining records and sets forth the minimum records keeping requirements and do not allow for deleting inaccurate information. Rather, the amendment to the medical records should be made on the date the error is corrected referring back to the incorrect information. A line may be drawn through the incorrect information with a marginal note explaining that it is erroneous information with reference to the records page at which the amended information may be found.

The Practice may deny a patient's request for amendment if the Privacy Office determines that the information was not created by the Practice, is not part of the patient's chart generated by the Practice, or is accurate and complete.

The request for amendment of information and the response should be placed in the patient's file and kept for at least six years.

STEP NINE - PATIENT COMPLAINTS:

The Notice of Privacy Practices notifies the patients of their right to make a complaint regarding the Practices' privacy policies, procedures and practices or failure to protect a patient's Protected Health Information. The complaint must be in writing and submitted to the Privacy Officer. A form for filing a complaint is found at page 41. The Privacy Officer will within 15 days of receiving a complaint 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 the Protected Health Information.

The patients are advised in the Notice of Privacy Practices that they may complain to the Practice or to the Office of Civil Rights, U.S. Department of Health and Human Services or to the Florida Attorney General if they believe that their privacy rights have been violated. Florida Statute 456.057 (17) authorizes the Florida Attorney General to enforce violations of Florida Statute 456.057 with fines of up to \$5,000 per violation.

The complaint and response shall be kept for a minimum of six years.

STEP TEN - CONFIDENTIAL COMMUNICATIONS:

Patients may have special requests about receiving information, such as appointment reminders or tests results. Some patients may not want telephone messages left about appointments or health information, nor discussions with any family members, nor post cards sent. The Notice of Privacy Practices places patients on notice that the Practice will be mailing post card reminders, leaving voice mail messages about appointments and may discuss patient information with family members. Patients should be asked whether they want stricter confidentiality regarding communications. Fill in the name of the Practice in the Request for Special Confidential Communications form found at page 42 and print it out to have available for patients. A patient who wants more strict communication procedures should be given a copy of the form the completed copy of which should be kept in the patient's file.

STEP ELEVEN - PROTECTING PATIENT INFORMATION STORED ON COMPUTERS:

The HIPAA regulations require any practice that uses a computer to store Protected Health Information to comply with the Electronic Transaction. At page 43 is a policy entitled *Electronic Transfer of Protected Patient Information Privacy Practice* that is adopted by the Practice Resolution Adoption of HIPAA Privacy Compliance Manual. Fill in the name of the Practice on that form. All electronic claims or Protected Health Information that is transmitted over the Internet must be transmitted using software that complies with the HIPAA regulations and that encrypts and protects the Protected Patient Information. Follow the *Electronic Transfer of Protected Patient Information Privacy Practice*.

STEP TWELVE - BUSINESS ASSOCIATE AGREEMENTS: Fill in the name of the Practice in the Business Associate Agreement form found at pages 44-49. Business associates include technicians who work on the Practice's computers on which PHI is stored, transcriptionists, billing services, clearing houses, attorneys, accountants, collection agencies, etc., WHO HAVE ACCESS TO PHI. A person who does not have access to PHI does not have to sign an agreement. Other doctors or employees in the Practice are not business associates and are covered by the confidentiality requirements of HIPAA and Florida Statute 456.057. Janitors are not business associates. Give a copy of the Business Associate Agreement to each such person who has access, to sign and maintain a copy of the signed agreements at the end of this manual. Maintain a file with a copy of all BAAs and a log of them, found at page 50.

STEP THIRTEEN - EMPLOYEE TRAINING: Train employees and new employees as they are hired so that they understand the privacy procedures: This can be done by having each employee read the FCA HIPAA Compliance Manual including the Notice of Privacy Practices found in the manual and by sending employees to the FCA conventions for additional training. Each doctor should meet with staff to discuss the office policies for protection of patient information. There is a Privacy Training and Education Log at page 51. Enter the employees' names, their dates of training, the description of the training, the training hours and the person or company providing the training. Maintain the log in the three ring binder as part of the compliance manual and keep for at least six years. A copy of the log may, also, be kept in employees' personnel file as their names are logged.

Advise employees that violations of the provisions of this manual will be subject to discipline such as a written warning placed in the employee's personnel file, a period of probation, mandatory additional training on maintaining the privacy of Protected Health Information, demotion or reassignment of position or termination. The Privacy Officer will maintain a record of the discipline for at least six years.

Employees should be encouraged to report any suspected privacy violations to the Privacy Officer. The employees should be assured that no retaliation will be taken against an employee for reporting suspected violations. The Privacy Officer will investigate reported suspected privacy violations and take reasonable steps to ensure that similar violations do not occur in the future.

STEP FOURTEEN - OFFICE WALK THROUGH:

As the last step in compliance, walk through the office taking note of places where Protected Health Information may be "leaked." Check computer monitor screens to determine whether patients can read the screens or others unauthorized to view Protected Health Information. Check fax machine and copy machine stations, patient records storage areas, and other places at which Protected Health Information is kept to determine whether patients can read the PHI or others unauthorized to view Protected Health Information. Take steps to correct "leaks."

Compliance Checklist

Verify:

- That the Resolution of Adoption of the Compliance Manual is signed and in the three ring manual binder;
- Privacy Notice is posted in waiting room;
- Privacy Officer is appointed and understands duties;
- That each patient file has a signed, up to date Notice of Privacy Practices and Acknowledgment of Receipt of Notice of Privacy Practices;
- That a log of disclosures of patient records to third parties is maintained in patient files;
- That each Business Associate has signed a Business Associate Agreement;
- That the Business Associate Agreements are all in one file with a log of all of them;
- That computer operators log off when leaving a computer unattended for more than a few moments;
- That any wireless network used in the Practice is password secured;
- Maintain a log of all passwords used by any physician or employee to access PHI. Periodically change the passwords.
- That any wireless device that accesses PHI is secure from theft.
- That software used to access and transmit PHI is up to date, including any encryption software.
- That the office HIPAA manual is in a safe secure place.
- That policies, standards, and procedures to protect the confidentiality and security of the medical records have been adopted and in the three ring manual binder; and
- That employees have been trained in all the policies, standards and procedures and that their dates of training are entered into the log.

**PRACTICE RESOLUTION
ADOPTION OF HIPAA PRIVACY COMPLIANCE MANUAL**

WHEREAS, Dr. Stephen L. Moleski's office desires to comply with the privacy protection requirements of the HIPAA Privacy Rule, the Security Rule, the HITECH Act, the Omnibus Rule and Florida Statutes 456.057; and

WHEREAS, the Practice has reviewed the Privacy Manual; and

WHEREAS, the Privacy Manual is intended to satisfy fully the requirements of the HIPAA Privacy Rule, the Security Rule, the HITECH Act and Regulation and Florida Statutes 456.057;

NOW THEREFORE, BE IT RESOLVED, that Dr. Stephen L. Moleski's Office hereby approves of the adoption of this HIPAA Privacy Compliance Manual and all policies therein to protect Protected Health Information, effective October 4, 2013, with the expectation that all employees, including those with an ownership interest in this Practice, will be instructed in their respective duties under this Manual and will comply fully therewith.

Date: October 4, 2013

By: Edye M. Coxwell

APPOINTMENT OF A PRIVACY OFFICER AND CONTACT PERSON

WHEREAS, Dr. Stephen L. Moleski's Office, having adopted this HIPAA Privacy Compliance Manual; and

WHEREAS, the Manual requires the appointment of a Privacy Officer and Contact Person; and

NOW THEREFORE, BE IT RESOLVED, that

Edye Coxwell is to be the Privacy Officer and Contact Person of this Practice beginning ~~October~~4,2013, and continuing until changed in accordance with this HIPAA Privacy Compliance Manual; and

BE IT FURTHER RESOLVED, that the Privacy Officer / Contact Person will vigorously carry out the duties set forth in this Manual and that all employees of this Practice will be informed of the importance of adherence to this HIPAA Privacy Compliance Manual and the importance of their cooperation with the Privacy Officer/Contact Person.

Date: October 4, 2013

By: Stephen L. Moleski, D. C.

Dr. Stephen L. Moleski
NOTICE OF PRIVACY PRACTICES
THIS NOTICE DESCRIBES HOW MEDICAL
INFORMATION ABOUT YOU
MAY BE USED AND DISCLOSED AND HOW YOU CAN
GET ACCESS TO
THAT INFORMATION.

PLEASE REVIEW THIS NOTICE CAREFULLY.

This Practice is committed to maintaining the privacy of your protected health information ("PHI"), which includes information about your health condition and the care and treatment you receive from the Practice. The creation of a record detailing the care and services you receive helps this office to provide you with quality health care. This Notice details how your PHI may be used and disclosed to third parties. This Notice also details your rights regarding your PHI. The privacy of PHI in patient files will be protected when the files are taken to and from the Practice by placing the files in a box or brief case and kept within the custody of a doctor or employee of the Practice authorized to remove the files from the Practice's office. It may be necessary to take patient files to a facility where a patient is confined or to a patient's home where the patient is to be examined or treated.

NO CONSENT REQUIRED

The Practice may use and/or disclose your PHI for the purposes of:

- (a) Treatment - In order to provide you with the health care you require, the Practice will provide your PHI to those health care professionals, whether on the Practice's staff or not, directly involved in your care so that they may understand your health condition and needs. For example, a physician treating you for a condition or disease may need to know the results of your latest physician examination by this office.
- (b) Payment - In order to get paid for services provided to you, the Practice will provide your PHI, directly or through a billing service, to appropriate third party payers, pursuant to their billing and payment requirements. For example, the Practice may need to provide the Medicare program with information about health care services that you received from the Practice so that the Practice can be properly reimbursed. The Practice may also need to tell your insurance plan about treatment you are going to receive so that it can determine whether or not it will cover the treatment expense.

- (c) Health Care Operations - In order for the Practice to operate in accordance with applicable law and insurance requirements and in order for the Practice to continue to provide quality and efficient care, it may be necessary for the Practice to compile, use and/or disclose your PHI. For example, the Practice may use your PHI in order to evaluate the performance of the Practice's personnel in providing care to you.

1. The Practice may use and/or disclose your PHI, without a written Consent from you, in the following additional instances:

(a) De-identified Information - Information that does not identify you and, even without your name, cannot be used to identify you.

(b) Business Associate - To a business associate if the Practice obtains satisfactory written assurance, in accordance with applicable law, that the business associate will appropriately safeguard your PHI. A business associate is an entity that assists the Practice in undertaking some essential function, such as a billing company that assists the office in submitting claims for payment to insurance companies or other payers.

(c) Personal Representative - To a person who, under applicable law, has the authority to represent you in making decisions related to your health care.

(d) Emergency Situations -

- (i) for the purpose of obtaining or rendering emergency treatment to you provided that the Practice attempts to obtain your Consent as soon as possible; or
- (ii) to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating your care with such entities in an emergency situation.

(e) Communication Barriers - If, due to substantial communication barriers or inability to communicate, the Practice has been unable to obtain your Consent and the Practice determines, in the exercise of its professional judgment, that your Consent to receive treatment is clearly inferred from the circumstances.

(f) Public Health Activities - Such activities include, for example, information collected by a public health authority, as authorized by law, to prevent or control disease and that does not identify you and, even without your name, cannot be used to identify you.

(g) Abuse, Neglect or Domestic Violence - To a government authority if the Practice is required by law to make such disclosure. If the Practice is authorized by law to make such a disclosure, it will do so if it believes that the disclosure is necessary to prevent serious harm.

(h) Health Oversight Activities - Such activities, which must be required by law, involve government agencies and may include, for example, criminal investigations, disciplinary actions, or general oversight activities relating to the community's health care system.

(i) Judicial and Administrative Proceeding - For example, the Practice may be required to disclose your PHI in response to a court order or a lawfully issued subpoena.

(j) Law Enforcement Purposes - In certain instances, your PHI may have to be disclosed to a law enforcement official. For example, your PHI may be the subject of a grand jury subpoena. Or, the Practice may disclose your PHI if the Practice believes that your death was the result of criminal conduct.

(k) Coroner or Medical Examiner - The Practice may disclose your PHI to a coroner or medical examiner for the purpose of identifying you or determining your cause of death.

(l) Organ, Eye or Tissue Donation - If you are an organ donor, the Practice may disclose your PHI to the entity to whom you have agreed to donate your organs.

(m) Research - If the Practice is involved in research activities, your PHI may be used, but such use is subject to numerous governmental requirements intended to protect the privacy of your PHI and that does not identify you and, even without your name, cannot be used to identify you.

(n) Avert a Threat to Health or Safety - The Practice may disclose your PHI if it believes that such disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the disclosure is to an individual who is reasonably able to prevent or lessen the threat.

(o) Workers' Compensation - If you are involved in a Workers' Compensation claim, the Practice may be required to disclose your PHI to an individual or entity that is part of the Workers' Compensation system.

(p) Disclosure of immunizations to schools required for admission upon your informal agreement.

APPOINTMENT REMINDER

The Practice may, from time to time, contact you to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to you. The following appointment reminders are used by the Practice: a) a postcard mailed to you at the address provided by you; and b) telephoning your home and leaving a message on your answering machine or with the individual answering the phone.

DIRECTORY/SIGN-IN LOG

The Practice maintains a directory of and sign-in log for individuals seeking care and treatment in the office. Directory and sign-in log are located in a position where staff can readily see who is seeking care in the office, as well as the individual's location within the Practice's office suite. This information may be seen by, and is accessible to, others who are seeking care or services in the Practice's offices.

FAMILY/FRIENDS

The Practice may disclose to your family member, other relative, a close personal friend, or any other person identified by you, your PHI directly relevant to such person's involvement with your care or the payment for your care unless you direct the Practice to the contrary. The Practice may also use or disclose your PHI to notify or assist in the notification (including identifying or locating) a family member, a personal representative, or another person responsible for your care, of your location, general condition or death. However, in both cases, the following conditions will apply:

- (a) If you are present at or prior to the use or disclosure of your PHI, the Practice may use or disclose your PHI if you agree, or if the Practice can reasonably infer from the circumstances, based on the exercise of its professional judgment that you do not object to the use or disclosure.
- (b) If you are not present, the Practice will, in the exercise of professional judgment, determine whether the use or disclosure is in your best interests and, if so, disclose only the PHI that is directly relevant to the person's involvement with your care.

AUTHORIZATION

Uses and/or disclosures, other than those described above, will be made only with your written Authorization.

YOUR RIGHTS

1. You have the right to:

(a) Revoke any Authorization and/or Consent, in writing, at any time. To request a revocation, you must submit a written request to the Practice's Privacy Officer.

(b) Request restrictions on certain use and/or disclosure of your PHI as provided by law. However, the Practice is not obligated to agree to any requested restrictions. To request restrictions, you must submit a written request to the Practice's Privacy Officer. In your written request, you must inform the Practice of what information you want to limit, whether you want to limit the Practice's use or disclosure, or both, and to whom you want the limits to apply. If the Practice agrees to your request, the Practice will comply with your request unless the information is needed in order to provide you with emergency treatment.

(c) Receive confidential communications or PHI by alternative means or at alternative locations. You must make your request in writing to the Practice's Privacy Officer. The Practice will accommodate all reasonable requests.

(d) Inspect and obtain a copy your PHI as provided by 45 CFR 164.524. To inspect and copy your PHI, you are requested to submit a written request to the Practice's Privacy Officer. The Practice can charge you a fee for the cost of copying, mailing or other supplies associated with your request

(e) Amend your PHI as provided by 45 CFR 164.528. To request an amendment, you must submit a written request to the Practice's Privacy Officer. You must provide a reason that supports your request. The Practice may deny your request if it is not in writing, if you do not provide a reason in support of your request, if the information to be amended was not created by the Practice (unless the individual or entity that created the information is no longer available), if the information is not part of your PHI maintained by the Practice, if the information is not part of the information you would be permitted to inspect and copy, and/or if the information is accurate and complete. If you disagree with the Practice's denial, you will have the right to submit a written statement of disagreement.

(f) Receive an accounting of disclosures of your PHI as provided by 45 CFR 164.528. The request should indicate in what form you want the list (such as a paper or electronic copy)

(g) Receive a paper copy of this Privacy Notice from the Practice upon request to the Practice's Privacy Officer.

(h) Receive notice of any breach of confidentiality of your PHI by the Practice.

(i) Prohibit report of any test, examination or treatment to your health plan or anyone else for which you pay in cash or by credit card.

(j) Complain to the Practice or to the 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 or to the Florida Attorney General, Office of the Attorney General, PL-01 The Capitol, Tallahassee, FL 32399-1050, 850 414-3300 if you believe your privacy rights have been violated. To file a complaint with the Practice, you must contact the Practice's Privacy Officer. All complaints must be in writing.

(k) Request copies of your PHI in electronic format.

To obtain more information on, or have your questions about your rights answered; you may contact the Practice's Privacy Officer, Edey Coxwell, at 878-5636 or via email at drmoleski@moleskidc.com

PRACTICE'S REQUIREMENTS

1. The Practice:

- (a) Is required by federal law to maintain the privacy of your PHI and to provide you with this Privacy Notice detailing the Practice's legal duties and privacy practices with respect to your PHI.
- (b) Is required by State law to maintain a higher level of confidentiality with respect to certain portions of your medical information that is provided for under federal law. In particular, the Practice is required to comply with the following State statutes:

Section 381.004 relating to HIV testing, Chapter 384 relating to sexually transmitted diseases and Section 456.057 relating to patient records ownership, control and disclosure.
- (c) Is required to abide by the terms of this Privacy Notice.
- (d) Reserves the right to change the terms of this Privacy Notice and to make the new Privacy Notice provisions effective for your entire PHI that it maintains.
- (e) Will distribute any revised Privacy Notice to you prior to implementation.
- (f) Will not retaliate against you for filing a complaint.

QUESTIONS AND COMPLAINTS

You may obtain additional information about our privacy practices or express concerns or complaints to the person identified below whom is the Privacy Officer and Contact person appointed for this practice. The Privacy Officer is Edye Coxwell.

You may file a complaint with the Privacy Officer if you believe that your privacy rights have been violated relating to release of your protected health information. You may, also, submit a complaint to the Department of Health and Human Services the address of which will be provided to you by the Privacy Officer. We will not retaliate against you in any way if you file a complaint.

EFFECTIVE DATE

This Notice is in effect as of 10/04/13.

**ACKNOWLEDGMENT OF RECEIPT
OF
NOTICE OF PRIVACY PRACTICES**

I acknowledge that I was provided a copy of the Notice of Privacy Practices and that I have read them or declined the opportunity to read them and understand the Notice of Privacy Practices. I understand that this form will be placed in my patient chart and maintained for six years.

Patient Name (please print)

Date

Parent, Guardian or Patient's legal representative

Signature

THIS FORM WILL BE PLACED IN THE PATIENT'S CHART AND MAINTAINED FOR SIX YEARS.

List below the names and relationship of people to whom you authorize the Practice to release PHI.

_____	_____
_____	_____
_____	_____

PATIENT'S REQUEST FOR COPIES OF RECORDS

I hereby request a copy of my patient records and x-rays from Dr. Moleski's Office. I request the copies: (check one) on paper _____ in electronic format _____ by email transmission to (fill in email address) _____ . I understand that Section 460.413 (1) (m), Florida Statutes, and Board of Chiropractic Medicine Rule 64B2-17.006 require chiropractic physicians to retain records and x-rays for at least four years. Therefore, a chiropractic physician receiving a request for a patient's x-ray within that four-year period must retain the x-ray and provide a copy of it in lieu of the original x-ray. I, further, understand that Section 456.057 (18), Florida Section 457.057 (16), Florida Statutes, authorizes a health care practitioner or patient records owner furnishing copies of reports or records or making the reports or records available for digital scanning pursuant to this section to charge no more than the actual cost of copying, including reasonable staff time, or the amount specified in administrative rule by the appropriate board, or the department when there is no board. The Board of Chiropractic Medicine Rule 64B-17.0055, Florida Administrative Code, authorizes chiropractic physicians to charge patients \$1.00 per page for the first 25 pages, and 25 cents for each page in excess of 25 pages. The Board of Chiropractic Medicine Rule defines the reasonable costs of reproducing x-rays, and such other special kinds of records as the actual costs. The phrase "actual costs" means the cost of the material and supplies used to duplicate the record, as well as the labor costs and overhead costs associated with such duplication. The Board of Chiropractic Medicine Rule 64B-17.0055, Florida Administrative Code, authorizes chiropractic physicians to charge people who are not patients authorized to seek copies of my patient records \$1.00 per page. I understand that the HIPAA regulations authorize the practice to charge the cost of labor and hardware onto which the records are electronically copied unless the Board of Chiropractic Medicine sets lower costs. I understand that there is no cost for transmitting the electronic records by email.

Patient's or Patient's Legal Representative's Signature

Date Signed

YOU MAY REFUSE TO SIGN THIS REQUEST.

DOCUMENTS FURNISHED TO PATIENT:

X-RAYS FURNISHED TO PATIENT:

DATE RECORDS OR X-RAYS FURNISHED TO PATIENT:

RELEASE OF PATIENT RECORDS AUTHORIZATION

I hereby authorize _____(name of practice) to release a copy of my patient records or x-rays containing protected health information to Dr. Moleski's office. This authorization is given pursuant to Florida Statute 456.057 and HIPAA regulations. I understand that Florida Statute 456.057 (12) makes clear that any third party to whom records are disclosed is prohibited from further disclosing any information in the medical record without the expressed written consent of the patient or the patient's legal representatives.

Patient's or Patient's Legal Representative's Signature

Patient's Date of Birth

Date Signed

Specific description of information to be disclosed:

ACCOUNTING OF DISCLOSURES FORM

There is recorded on these form any and all disclosures of information contained in the medical record to any third party, including the purpose of the disclosure, required to be maintained by Florida Statute 456.057 (12) and provided to a patient upon request pursuant to HIPAA regulations. This form shall be maintained as part of the patients' records pursuant to Florida Statute 456.057 (12). A copy of this form shall be provided to any patient requesting an accounting or a copy of their patient records. This form will be maintained as part of the medical records for at least six years.

Signature of Privacy Officer

Date Provided to Patient

DATE OF DISCLOSURE	PERSON / ENTITY TO WHOM DISCLOSURES WERE MADE	RECORD OF INFORMATION DISCLOSED	REASON FOR DISCLOSURE
-----------------------	--	---------------------------------------	--------------------------

REQUEST FOR ACCOUNTING OF DISCLOSURES OF PROTECTED PATIENT INFORMATION

I hereby request an accounting all disclosures of my patient protected information.

Patient's or Patient's Legal Representative's Signature

Patient's Date of Birth

Date Request is signed

REQUEST FOR CORRECTION OR AMENDMENT OF HEALTH INFORMATION

Patient Name: _____ Date of Birth: _____

Patient's Address: _____

Patient's Phone Number: _____

Date of Entry to be Amended: _____

Type of Entry to be Amended: _____

Statement as to why the entry is incorrect or incomplete and what the entry should state to be more complete or accurate.

Please list those people to whom we have sent the erroneous information and whom you would like to have a copy of the amended information sent:

Name: _____

Address: _____

Name: _____

Address: _____

Patient's or Patient's Legal Representative's Signature Date _____

For use by the Privacy Officer

Date received _____ Amendment ___ Accepted ___ Denied

Reason for denial:

- PHI was not created by the Practice
- PHI is not part of patient's designated record set
- PHI is accurate and complete

Additional comments:

Signature of Privacy Officer: _____ Date: _____

Signature of Physician: _____ Date: _____

PATIENT COMPLAINT FORM

PATIENT NAME: _____ PATIENT'S BIRTH DATE: _____

NAME OF PERSON SUBMITTING COMPLAINT IF OTHER THAN PATIENT:

RELATIONSHIP TO PATIENT: _____

DATE OF OCCURRENCE: _____

NAME OF PRACTICE EMPLOYEE INVOLVED IN MATTER: _____

DESCRIPTION OF OCCURRENCE AND REASON FOR COMPLAINT: _____

DESCRIBE THE ACTION YOU WANT THIS OFFICE TO TAKE RELATING TO THIS OCCURRENCE:

Signature

DATE

FOR USE BY PRACTICE OFFICER ONLY

Description of action taken to address complaint: _____

Signature of Privacy Officer: _____

Date: _____

**REQUEST FOR SPECIAL CONFIDENTIAL COMMUNICATIONS
PROCEDURES**

I hereby request that Dr. Moleski's Office _____
request that all written communications to be mailed only to the following address:

I hereby request that Dr. Moleski's Office _____
request that all telephone calls placed to me only be placed to: _____.

I hereby request that Dr. Moleski's Office _____
request that no voice mail messages be left on the above listed or any other
telephone listings relating to me.

Patient's Signature

Patient's Date of Birth

For Use by Privacy Officer Only

Practice: ___ Accepts ___ Denies

Signature of Privacy Officer: _____

Date: _____

ELECTRONIC TRANSFER OF PROTECTED PATIENT INFORMATION PRIVACY PRACTICE

The Dr. Moleski's Office seeks to protect the privacy of Protected Health Information stored on computers of the Dr. Moleski's Office or transmitted via the internet.

Only authorized employees shall have access to computers on which Protected Patient Information is stored. All computers will be protected with a password. Only authorized employees may use a password to access computers. The password will be periodically changed and changed any time an authorized employee leaves the Practice's employ.

Only the owners of the practice will be authorized to take out of the Practice's premises back up discs or flash drives onto which Protected Patient Information has been copied. The owner will take appropriate steps to protect the information on the discs or flash drives from unauthorized disclosure. Back up data will be stored in a secure place.

Any electronic claims that may be filed using software that is approved for electronic transmissions of Protected Health Information and which protects the privacy of such information as it becomes available.

The Practice will make certain that any billing services used by the Practice to electronically file claims on behalf of the Practice have a policy adopted that protects Protected Health Information and that uses software that is approved for electronic transmissions of Protected Health Information and which protects the privacy of such information.

BUSINESS ASSOCIATE AGREEMENT

Compliant with HiTech Act of 2009

Definitions

Terms used, but not otherwise defined in this Agreement shall have the same meaning as those terms in the Privacy Rule.

Examples of specific definitions:

- a. **HIPAA Rules.** “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.
- b. **Breach of HIPAA and HiTech Act.** Section 13400(1) of the HiTech Act defines “breach” to mean, generally, the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information.
- c. **Business Associate.** “Business Associate” shall mean (name of contractor)
- d. **Covered Entity.** “Covered Entity” shall mean (name of practice).
- e. **Disclosure of Breach.** Section 13402(b) of the Act requires a business associate of a covered entity that accesses, maintains, retains, modifies, records, destroys, or otherwise holds, uses, or discloses unsecured protected health information to notify the covered entity when it discovers a breach of such information, so that the covered entity can notify affected patients.
- f. **Individual.** “Individual” 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).
- g. **HiTech Act of 2009** means Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009 (ARRA) that was enacted on February 17, 2009.

- h. **Law Enforcement official.** “Law enforcement official” means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:
 - (1) Investigate or conduct an official inquiry into a potential violation of law; or
 - (2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.
- b. **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.
- c. **Protected Health Information.** “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 CFR § 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
- d. **Required By Law.** “Required By Law” shall have the same meaning as the term “required by law” in 45 CFR § 164.501.
- e. **Secretary.** “Secretary” shall mean the Secretary of the Department of Health and Human Services or his designee.
- f. **Unsecured Protected Health Information.** Section 13402(h) of the HiTech Act defines “unsecured protected health information” as “protected health information that is not secured through the use of a technology or methodology.

Obligations and Activities of Business Associate

1. Business Associate agrees not to use or disclose Protected Health Information other than as permitted or required by this Agreement or as Required by Law.
2. Business Associate agrees to maintain all computers on which patient protected information is stored in a secure manner protected from access by anyone who is not entitled to access the Protected Health Information.
3. Business Associate agrees to transmit electronically Protected Health Information only in a secure manner by encryption or other secure manner.
4. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
5. Business Associate agrees 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.
6. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.
7. Business Associate agrees 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 Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.
8. Business Associate agrees to provide access, at the request of Covered Entity to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR § 164.524.
9. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity or an Individual.
10. Business Associate agrees to make 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, Covered Entity available to Covered Entity, for purposes of the Secretary determining Covered Entity compliance with the Privacy Rule. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

11. Business Associate agrees to provide to Covered Entity or an Individual, information collected in accordance with this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

Permitted Uses and Disclosures by Business Associate

General Use and Disclosure Provision

Purpose:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of Covered Entity for the following purposes, provided that such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity: To provide information to law enforcement officials and to petition such officials for related investigations.

Obligations of Covered Entity

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

- a. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity 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. Covered Entity shall 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 use or disclosure of Protected Health Information.
- c. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity 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.

Permissible Requests by Covered Entity

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

Term and Termination

- a. **Term.** The Term of this Agreement shall be effective as of _____, 20 , and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity. Or, if it is infeasible 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 Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:
 1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;
 2. Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or
 3. If neither termination nor cure is feasible, Covered Entity 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 Covered Entity, or created or received by Business Associate on behalf of Covered Entity. 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.

In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon notification that return or destruction of Protected Health Information is infeasible, 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 infeasible, for so long as Business Associate maintains such Protected Health Information.

Miscellaneous

- a. **Regulatory References.** A reference in this Agreement to a section in the Privacy 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 Covered Entity to comply with the requirements of the Privacy 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 of this Agreement shall survive the termination of this Agreement.
- d. **Interpretation.** Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

Contractor

By (person signing for contractor)

Date

_____ CHIROPRACTIC CENTER

By Dr.

Date

Prepared by Paul Watson Lambert, General Counsel, Florida Chiropractic Association
This Business Associate Agreement is intended for use only by members of the Florida Chiropractic Association.

Log of Business Associate Agreements

Name of Business Associate	Reason for Access to PHI	Expected Frequency of Access to PHI	Date Signed
----------------------------	--------------------------	-------------------------------------	-------------

PRIVACY TRAINING AND EDUCATION LOG

DATE OF TRAINING	NAME OF EMPLOYEE	DESCRIPTION OF TRAINING	TRAINING HOURS	PERSON OR COMPANY PROVIDING TRAINING
_____	_____	_____	_____	_____

NOTICE TO INDIVIDUAL PATIENT OF BREACH OF PROTECTED PATIENT INFORMATION FOR BREACH OF FEWER THAN 10 PATIENTS

Send by U.S. Postal Service or other delivery service or email, if the patient has elected to receive information by email, the notice below. In the event that the contact information out-of-date for one or more of the ten patients post the notice on the practice's web page for 90 days. A personal representative or next of kin should be contacted in the instance the patient is deceased.

NOTICE OF BREACH OF YOUR PROTECTED PATIENT INFORMATION

(Name of practice) discovered on (date) that the confidentiality of your Protected Patient Information was breached. (State the suspected date of the breach or that the date of the breach is unknown. Describe the types of unsecured PHI that were involved in the breach, whether the full name, home address, Social Security number, date of birth, account number, diagnosis, disability code, or other types of information were involved.)

(Describe: 1) any steps individuals should take to protect themselves from harm resulting from the breach; 2) a brief description of what the practice is doing to investigate the breach, mitigate harm to individuals and protect against any further breaches; 3) contact procedures for individuals to ask questions or learn additional information, including a telephone number, an email address, web site or postal address.

NOTICE TO THE MEDIA OF BREACH OF MORE THAN 500 PATIENTS OF PHI

In the event that PHI of greater than 500 patients, the practice post the notice form below on the practice's web site and submit the notice to the local media without reasonable delay and no later than 60 days following discovery of the breach.

NOTICE OF BREACH OF PROTECTED PATIENT INFORMATION

(Name of practice) discovered on (date) that the confidentiality of Protected Patient Information of greater than 500 patients was breached. (State the suspected date of the breach or that the date of the breach is unknown. Describe the types of unsecured PHI that were involved in the breach, whether the full name, home address, Social Security number, date of birth, account number, diagnosis, disability code, or other types of information were involved.)

(Describe: 1) any steps individuals should take to protect themselves from harm resulting from the breach; 2) a brief description of what the practice is doing to investigate the breach, mitigate harm to individuals and protect against any further breaches; 3) contact procedures for individuals to ask questions or learn additional information, including a telephone number, an email address, web site or postal address.

NOTICE TO THE SECRETARY OF HHS OF BREACH OF MORE THAN 500 PATIENTS OF PHI

The practice is required to notify the Secretary of the U.S. Department of Health and Human Services in the event that the PHI of greater than 500 patients has been breached. Below is a suggested wording of a letter notifying the Secretary.

Secretary's Name
Hubert Humphrey Building
200 Independence Avenue S.W.
Washington, D.C. 20201

Dear (Madam or Mister) Secretary:

(Name of practice) discovered on (date) that the confidentiality of Protected Patient Information of greater than 500 patients was breached. (State the suspected date of the breach or that the date of the breach is unknown. Describe the types of unsecured PHI that were involved in the breach, whether the full name, home address, Social Security number, date of birth, account number, diagnosis, disability code, or other types of information were involved.)

(Describe: 1) any steps individuals should take to protect themselves from harm resulting from the breach; 2) a brief description of what the practice is doing to investigate the breach, mitigate harm to individuals and protect against any further breaches; 3) contact procedures for individuals to ask questions or learn additional information, including a telephone number, an email address, web site or postal address.

NOTICE TO THE SECRETARY OF HHS OF BREACH OF FEWER THAN 500 PATIENTS OF PHI

The practice is required to maintain a log of breaches of PHI involving fewer than 500 patients. The practice is required to submit the log to the Secretary of the U.S. Department of Health and Human Services no later than 60 days after the end of the calendar year in which the breaches were discovered. Below is a suggested wording of a log notifying the Secretary.

LOG OF BREACHES OF PHI DURING THE CALENDAR YEAR OF 20XX

Date of Discovery	Date of Breach (If known)	Number of Patients	Date Patients Notified	Action Taken
-------------------	------------------------------	--------------------	------------------------	--------------

Mail the log to the Secretary at the address above.