Back To Chiropractic Continuing Education Seminars
HIPAA Made Easy – 2 Hours

Welcome to Back To Chiropractic Online CE exams:
This course counts toward your California Board of Chiropractic Examiners CE.
(also accepted in other states, check our website or with your Chiropractic State Board)

The California Board requires that you complete all of your CE hours BEFORE the end of your Birthday month. We recommend that you send your chiropractic license renewal form and fee in early to avoid any issues.

Exam Process: Read all instructions before starting!
1. You must register/pay first. If you haven't, please return to: backtochiropractic.net
2. Open a new window or a new internet tab & drag it so it's side-by-side next to this page.
3. On the new window or new tab you just opened, go to: backtochiropractic.net website.
4. Go directly to the Online section. DON'T register again.
5. Click on the Exam for the course you want to take. No passwords needed.
6. Follow the Exam instructions.
7. Upon passing exam (70%), you'll be able to immediately download your certificate, and it'll also be emailed to you. If you don't pass, you must repeat the exam.

Please retain the certificate for 5 years. DON'T send it to the state board.
If you get audited and lose your records, I'll have a copy.

I'm always a phone call away... 707.972.0047 or email: marcusstrutzdc@gmail.com

Marcus Strutz, DC
Back To Chiropractic CE Seminars
33000 North Highway 1
Ft Bragg CA 95437

HIPAA Made Easy

Online Class Notes
Author - Steven C Eggleston, DC, Esq.
Back To Chiropractic Seminars

General Instructions

There are 11 pages of notes for this class PLUS an appendix that contains a sample Business Associate Agreement that you can modify and use in your practice. ONLY THE FIRST 11 PAGES WILL BE TESTED FOR THIS CLASS. The appendix is ONLY for your use and will NOT be tested.

Glossary of Terms

HIPAA – Health Insurance Portability and Accountability Act of 1996
PHI – Protected Health Information
ePHI – electronically stored Protected Health Information
BA – Business Associate(s).
BAA – Business Associate Agreement
CEs – Covered Entities. Any organization subject to the HIPAA law(s)
NPP – Notice of Privacy Practices Form
OCR – Office of Civil Rights. The HHS (Health & Human Services) department that enforces HIPAA
CMS – Centers for Medicare & Medicaid Services
ONC – Office of the National Coordinator for Health Information Technology
ARRA HITECH ACT – The statute passed by Congress defining criminal and civil penalties as well as enforcement methods. It also added Business Associate requirements.
NHI – National Health Plan Identifier. An identifier of plans and payers for CMS
NPI – National Provider Identifier
EIN – Employer Identification Number
NIST Standards – National Institute of Standards and Technology is a division of the U.S. Department of Commers which sets security standards for eCommerce

The Purpose(s) of HIPAA

HIPAA was created because of computers. Its purpose is protect a patient's medical records from fraud and theft since computers in 1996 were becoming the new method of storage of sensitive patient information. HIPAA was not needed when all your patient's medical records were on paper in a file cabinet in your office. Computers can be hacked or stolen and your patient's medical data could be used for blackmail or to embarrassment by making it public. HIPAA and its follow up laws created rules to prevent this in the age of computers.

HIPAA is evolving to address advances in computer technology as well as addressing issues that were unforeseen in 1996. Business Associates is one of the most common areas where Protected Health Information (PHI) was getting outside of the doctor's office and, thus, privacy of that data was being frequently compromised. HIPAA's updated Business Associate Agreements require

that outside billing services and collection agencies keep your patients' data safe from fraud or theft.

Health Insurance Companies also have huge computer databases that store your patients' data which they obtain when you bill them for services. HIPAA made rules and standards to protect insurance companies from disclosing your patient's sensitive medical data. The basic premise is that once the "cat is out of the bag" and your patient's history of STDs or something else embarrassing gets out into the public, the patient can never restore the privacy that they expected from their doctor.

HIPAA was created in 1996 which is 8 years before Facebook and 11 years before the first iPhone was released. HIPAA is frequently amended to cover these new methods of data storage and sharing which are great threats to your patients' privacy.

BA – Business Associates MUST Keep Your Patient Data PROTECTED

Business Associates (BA) are entities who do not create, receive, manage or transmit PHI in the course of their main operations (like you do as a chiropractor), but who supply services and perform certain functions for chiropractors, during which they have ACCESS to the PHI of that chiropractor.

Examples:

1) Outside billing services
2) Practice management consultants
3) Collection agencies
4) Your I.T. guy that fixes your computers
5) Your CPA or accountant or bookkeeper
6) A Medical Transcriptionist who transcribes your reports or patient notes
7) Your practice management software company if they can access patient files remotely
8) An attorney that represents you in a Board Hearing or Malpractice case
9) Data transmission and storage companies (in case you store data "in the cloud")
10) Web-hosting services who might have access to PHI
11) Non-employee outside contractors who work in your office (someone you 1099)

If you use any of these services, your patients' PHI may be seen or heard about by someone you hire that works for you but is not an employee. In that case, you need a WRITTEN Business Associate Agreement (BAA) with each of them BEFORE you let them have access to PHI. If you don't get a BAA signed by your I.T. guy who comes in to fix your computer (or you take your computer out to a computer repair guy), you have a HIPAA violation on your hands.

Think about it this way. The I.T. guy knows more about your computer(s) than you do. He/she may be just installing Microsoft Office (not your practice management software) on your system but I.T. guys can look around on your computer or server at will. Making him/her sign a BAA makes them promise to NOT divulge to anyone any of your patients' PHI if they happen upon it while having access to your system. Suppose you live in a small town where everyone knows everybody's business. The I.T. guy logs in remotely or shows up in your office to fix a broken

CD disc drive. You don't make him/her sign a BAA. He happens to see your patient file of the mayor's daughter and find somewhere in your records the patient's M.D.'s records that you requested and received a copy. The I.T. guy sees that the mayor's daughter has an STD or had an abortion and finds that information too "juicy" to not tell his spouse or his friends. YOU are the one that gets in trouble by DHS for that HIPAA violation in your office. You get fined, not the I.T. guy. Unrelated to HIPAA, you might also get sued by the mayor's daughter and that would be a big mess, too.

Suppose you have a short in your electricity and have an electrician come into the front office to fix the outlet. While there, your front desk C.A. keeps working and PHI is on the screen while the electrician is working in that room. You need a SIGNED BAA by that electrician so he/she knows that you take privacy seriously and that anything seen on the computer is strictly private and cannot be leaked to anyone outside your office.

HOWEVER, the EXCEPTION to the BAA rule is someone like an electrician or janitorial service who would not, in general, come into contact with PHI and if so, such contact would be "incidental, if at all." You would not need a BAA for an electrician or janitor working in an area of your office where no reasonable person would expect that person to so see PHI on a computer screen, they could not access a password-protected computer in the room in which he/she is working and is not working in a room with an unlocked filing cabinet full of old patient files. Where access to PHI is unlikely, this falls under the "incidental, if at all" exception.

You also do NOT need a BAA for the Post Office who delivers your insurance billing forms to the insurance company, the financial institution that processes your patients' credit payments.

Take this seriously. Get a signed BAA from EVERY NON-EMPLOYEE that comes into your office for ANY reason. However, if you have patient authorization to send their records to another doctor, hospital, health insurance company or any other type of CE entity, you do not need a BAA for that situation.

The 5 Main HIPAA Rules

1) Privacy Rule

The Privacy Rule protects the PHI and medical records of individuals, with limits and conditions on the various uses and disclosures that can and cannot be made without patient authorization. This rule also gives every patient the right to inspect and obtain a copy of their records and request corrections to their file. There are specific forms that coincide with this rule: Request of Access to Protected Health Information (PHI); Notice of Privacy Practices (NPP) Form; Request for Accounting Disclosures Form; Request for Restriction of Patient Health Care Information; Authorization for Use or Disclosure Form; and the Privacy Complaint Form.

The Privacy Rule sets limits regarding the use of patient information when no prior authorization has been given by the patient. It also states that a patient and/or his/her representative have the right to obtain a copy of their health records and request corrections to errors contained therein. CEs have a 30 day *federal* deadline to respond to such requests. California has a shorter deadline

of only 15 days so California Chiropractors must give the patient (or perhaps the patient's personal injury attorney) the records and bills within 15 days under the Business and Professions Code.

EXCEPTIONS to the Privacy Rule:

1) Giving the patient their OWN data (not necessarily the spouse's data without authorization)
2) Someone authorized by the patient (e.g. a P.I. attorney who sends you a records request signed by the patient
3) Another health care professional who is treating the patient
4) Responding to investigations by DHS if they are investigating you for HIPAA violations

PATIENT-DIRECTED RESTRICTIONS RE: Privacy Rule

A patient may restrict what you disclose to certain people and institutions and you must follow the patient's wishes. For example a patient may ask you:

1) To not inform certain relatives about their condition(s)
2) To not inform their health insurance company about their treatments if the patient pays in full for those treatments him or herself
3) The method of communicating to the patient (i.e. no post cards, must use sealed envelopes, no messages left on their answering machine, that you not mail anything to their home address but, rather, to a P.O. Box or that you call their cell phone and not their home phone.

Basically, if you read your own HIPAA form that the patient has to sign, you will see the places where they can give you these patient-directed restrictions. Make sure to train your staff to READ the HIPAA form after the patient signs it and that person is in charge of compliance with the patient's requests.

2) Security Rule

The security rule defines and regulates the standards, methods and procedures related to the protection of electronic PHI on storage, accessibility and transmission. There are three safeguard levels of security. The Administrative safeguards deal with the assignment of a HIPAA security compliance team; the Technical safeguards deal with the encryption and authentication methods used to have control over data access, and the Physical safeguards deal with the protection of any electronic system, data or equipment within your facility and organization. The risk analysis and risk management protocols for hardware, software and transmission fall under this rule.

The Security Rule sets the *minimum* standards to safeguard ePHI. Any person within a CE or BA who can access, create, alter or transfer ePHI must follow these standards. Technical safeguards include encryption to NIST standards if the data goes outside the company's firewall.

The Security Rule also requires that workstation screens cannot be seen from a public area and require that someone in every CE be designated to conduct regular risk assessments and audits to identify any ways in which the integrity of PHI is threatened in your office and, if any are found, establish a policy in your office to fix the security risk. That can, of course, be you or anyone you designate. Just make sure that someone in your office "regularly" looks around your office for anything that might allow a patient's PHI to be seen by some other patient. Remember that sign in sheets that have a list of all your patients that day allows the patients at the end of the day to know the name of all your patients that day and that they have a chiropractic problem. That is arguably medical data combined with a Personal Identifier and, therefore a disclosure of PHI.

In the event of a Breach of your computer system where 500 or more patients' PHI has been breached, you must notify the Department of Health and Human Services (HHS) within 60 days of that breach. If fewer than 500 patients' data was breached, you must notify HHS within 60 days of the end of the calendar year in which the breach was experienced. You must also notify each patient whose PHI was compromised within 60 days. If more than 500 of your patients are affected by the breach, you have to send a media notice to a prominent news outlet serving your geographical area.

Security of your office computers is obviously VERY important under HIPAA laws. You may be complacent and think that nobody is going to hack into your office computers and get more than 500 of your patient files *but* the more common occurrence is that an office is broken into and the computers are stolen. That would be a breach of more than 500 of your patient files and you would have so notify the press and you don't want it on the 6:00 o'clock news that you did not keep your patient's data private. Consider an alarm system in your office to protect not only your possessions but also to keep your computers safe from a terrible breach of HIPAA laws that would require you to issue a press release about it.

OMNIBUS RULE: The HITECH act extended HIPAA protections to Bas and also prohibit using PHI for marketing or fundraising purposes without patient authorization.

3) Transactions Rule

This rule deals with the transactions and code sets used in HIPAA transactions, which includes ICD-9, ICD-10, HCPCS, CPT-3, CPT-4 and NDC codes. These codes must be used correctly to ensure the safety, accuracy and security of medical records and PHI.

4) Identifiers Rule

HIPAA uses three unique identifiers for covered entities who use HIPAA regulated administrative and financial transactions. These identifiers are: National Provider Identifier (NPI), which is a 10-digit number used for covered healthcare providers in every HIPAA administrative and financial transaction; National Health Plan Identifier (NHI), which is an identifier used to identify health plans and payers under the Center for Medicare & Medicaid Services (CMS); and the Standard Unique Employer Identifier, which identifies and employer entity in HIPAA transactions and is considered the same as the federal Employer Identification Number (EIN).

PHI can be "De-Identified" by making unlinking medical/chiropractic information from any of the 18 "Identifiers" listed below.

The 18 Personal Identifiers That MUST Be Protected

PHI or ePHI means that one of the following Personal Identifiers is COMBINED with health data. There is a difference between "somebody in the world" had a colonoscopy and "Mary Smith" had a colonoscopy. The 18 Personal Identifiers are:

Names or parts of names
Geographical identifiers
Phone number details
Details of Email addresses
Medical record numbers
Account details
Vehicle license plate details
Website URLs
Fingerprints, retinal and voice prints
IP address details
Device identifiers and serial numbers
Certificate or license numbers
Social Security details
Health insurance beneficiary numbers
Fax number details
Dates directly related to a person
Any other unique identifying characteristic

Someone could figure out exactly who had a colonoscopy by obtaining the CPT (procedure) code that a doctor billed or the ICD10 (diagnosis) code that was bills *along with* the patient's phone number, fax number, birth date, Social Security number, email address, car license plate, his home computer's IP address or even his iPhone's IP address. By combining any CPT or ICD10 code *with ANY* of these Personal Identifiers, a private investigator could easily figure out exactly who had a colonoscopy or who has syphilis or who had an abortion or many other potentially embarrassing things contained in your patient chart.

You need a *written* BAA contract between you and your outside billing service. Otherwise, you could be liable if your billing service inadvertently disclosed PHI to someone not authorized to see it. You also need a written BAA contract between you and any collection agency that you hire to collect money from patients. As a lawyer, I have seen doctors give a collection agency a CMS1500 billing form that has the patient's diagnosis codes and CPT codes on it as well as the patient's name, birthdate and many other Personal Identifiers. This was a serious breach of HIPAA's privacy rule for 2 reasons: (1) The doctor did NOT have a BAA with the collection agency; and (2) collection agencies are NOT allowed to have PHI. You are only allowed to tell them "Mary Smith owed me $800. Go get it for me." That statement does not contain PHI because there is no medical data disclosed. Remember, PHI or ePHI only exists when you combine medical data *and* a Personal Identifier.

NOTE: If you create a BAA on your Web Site or transmit it across the Internet (email) or a wireless network, be sure to use ENCRYPTION (end-to-end encryption is best) for that form.

5) Enforcement Rule

This rule is derived from the ARRA HITECH ACT provisions for violations that occurred before, on or after the February 18, 2015 compliance date. This expands the rules under HIPAA Privacy and Security, increasing the penalties for any violations. This addresses five main areas in regards to covered entities and business associates: Application of HIPAA security and privacy requirements; establishment of mandatory federal privacy and security breach reporting requirements; creation of new privacy requirements and accounting disclosure requirements and restrictions on sales and marketing; establishment of new criminal and civil penalties, and enforcement methods for HIPAA non-compliance; and a stipulation that all new security requirements must be included in all Business Associate contracts.

This rule sets the fines and how investigations are carried out. For example, if a violation is due to *ignorance*, a fine of up to $50,000 can be levied against the negligent doctor per violation. If the violation was willful (you knew about it, just let it happen and did not correct it within 30 days), a fine of $50,000 per offence is possible up to an annual maximum of $1,500,000.

The "final" Onmibus Rule was introduced in 2013 and provides a patient with even more power to control their own medical data. I suggest that if you have not already paid someone to come into your office and make sure you are compliant, hire one of these companies to do so but make sure to have a written, signed BAA with this company before you let them in. Also, double check to make sure your computer software company uses NIST standards to protect your patient data.

The Security Rule In Regard To Email Encryption Under HIPAA

The Security Rule applies to email messages because they are ePHI and travel/transit across the internet or wireless networks. One area of HIPAA that has resulted in some confusion is the difference between "required" and "addressable" security measures. Practically every safeguard of HIPAA is "required" unless there is a justifiable rationale not to implement the safeguard, or an appropriate alternative to the safeguard is put in place that achieves the same objective and provides an equivalent level of protection.

An instance in which the implementation of an addressable safeguard might be not required is the encryption of email. Emails containing ePHI – either in the body or as an attachment – only have to be encrypted if they are shared beyond a firewalled, internal server. If a healthcare group only uses email as an internal form of communication – or has an authorization from a patient to send their information unencrypted outside the protection of the firewall – there is no need to adopt this addressable safeguard.

The decision not to use email encryption will have to be backed up by a risk assessment and must be documented in writing. Other factors that may have to be considered are the organization's risk mitigation strategy and other security measures put in place to secure the

integrity of PHI. As a footnote to this particular section of HIPAA explained, the encryption of PHI at rest and in transit is recommended.

The Security Rule In Regard To HIPAA Password Requirements

HIPAA is vague when it comes to specific technologies and controls that should be applied to secure ePHI and systems that store health information, and this is certainly true for passwords.

Even though passwords are one of the most basic safeguards to prevent unauthorized accessing of data and accounts, there is little mention of passwords in HIPAA. The only HIPAA password requirements that are specified are that HIPAA-covered entities and their business associates must implement "Procedures for creating, changing, and safeguarding passwords."

Even though password requirements are not detailed in HIPAA, HIPAA covered entities should develop policies covering the creation of passwords and base those policies on current best practices. It is strongly recommended that healthcare organizations follow the advice of NIST when creating password policies.

While NIST has previously recommended the use of complex passwords, its advice on passwords has recently been revised. Highly complex passwords may be 'more secure' but they are difficult to remember. As a result, employees often write their passwords down. To avoid this, passwords should be difficult to guess but also memorable. The use of long passphrases rather than passwords is now recommended.

Generally, passwords should:

- Be a minimum of 8 characters up to 64 characters, with passphrases – memorized secrets – longer than standard passwords recommended.
- NIST advises against storing password hints as these could be accessed by unauthorized individuals and be used to guess passwords.
- A password policy should be implemented to prevent commonly used weak passwords from being set, such as 'password', '12345678', 'letmein' etc.
- NIST now recommends not forcing users to change their passwords frequently. A change should only be required infrequently or is there is very good reason for doing so – such as following a security breach.
- Multi-factor authentication should be implemented.
- NIST recommends salting and hashing stored passwords using a one-way key derivation function.

The Security Rule In Regard To HIPPA Compliant Text Messages

The Security Rule applies to text messages because they are ePHI and travel/transit across the internet or wireless networks. Text messages to patient must also be HIPPA compliant IF the CE creates, maintains, receives, forwards or transmits PHI. Obviously, a chiropractic office does some or all of these. There are HIPPA compliant texting apps available at a very reasonable cost so be sure to implement one of these in your chiropractic office and resist the temptation to just

text from your cell phone's text message program. Although I am not recommending any specific app or program (and receive no remuneration from any of these), here are some reputable healthcare messaging apps to consider when texting your patients: Klara, Backline, Luma Health, Health Engage or Well. There is also a different class of texting apps that can be used to communicate between the doctor and staff members. Some of them are: Zinc, TigerText Essentials, Notifyd or Spok, Some of these may be designed for large organizations and more costly, but this partial list is a starting point for you to investigate in case you are still texting your patients or staff using regular old text messages.

Summary of Basic HIPPA Do's and Don'ts

Do - treat patient personal information as you would want your own personal information to be treated.
Do – Go into a private office and close the door to discuss PHI on the telephone
Do – Train your staff to be careful on the phone at the front desk and NOT use patient names when scheduling appointments when other patients in the waiting room might overhear, "Hi Mary. Yes, I can make you an appointment for you and your son, John…"
Do – Keep patient data secure and respect your patient's right to privacy
Do – Use passwords that are not obvious, keep them in a secure place and change them regularly
Do – Keep your voice down when discussing patient finances, both in person and on the phone
Do – Have an office policy that the office manager (aka compliance officer) must register everybody's passwords and keep them in a safe, central location.

Don't – Use patient names in public areas (hallway, waiting room, elevator, bathroom)
Don't – Don't write passwords on the side of the computer
Don't – Don't use the same password for everything
Don't – Don't discuss personal issues in the presence of patients
Don't – Don't allow family members of office staff in the secure data areas of the office
Don't – Leave patient files or records laying around where non-staff can see them
Don't – Leave a non-password protected computer station on in a room where a patient could start looking things up when nobody is in the room

10 Examples of Common HIPAA Violations

1) Risk Analysis Failures

One of the most common HIPAA violations discovered by OCR is the failure to perform a comprehensive, organization-wide risk analysis. HIPAA requires covered entities and their business associates to conduct regular risk analyses to identify vulnerabilities to the confidentiality, integrity, and availability of PHI.

2) Risk Management Failures

All risks identified during the risk analysis must be subjected to a HIPAA-compliant risk management process and reduced to a reasonable and appropriate level. Risk management is

critical to the security of ePHI and PHI and is a fundamental requirement of the HIPAA Security Rule.

3) Lack of Encryption or Alternative Safeguards

While HIPAA does not demand the use of encryption, encryption is an addressable implementation specification and must be considered. The failure to use encryption or an alternative equivalent safeguard to ensure the confidentiality, integrity, and availability of ePHI has resulted in many healthcare data breaches.

4) Security Awareness Training Failures

HIPAA requires covered entities and business associates to implement a security awareness training program for all members of the workforce, including management. Training should be provided regularly and the frequency should be determined by means of a risk analysis.

5) Improper Disposal of PHI

When PHI or ePHI is no longer required it must be disposed of securely in a manner that ensures PHI is "unreadable, indecipherable, and otherwise cannot be reconstructed." Paper records should be shredded, burnt, pulped, or pulverized, while electronic media should be cleared, purged, degaussed, or destroyed.

6) Impermissible Disclosures of PHI

An impermissible disclosure of PHI is a disclosure not permitted under the HIPAA Privacy Rule. This includes providing PHI to a third party without first obtaining consent from a patient and 'disclosures' when unencrypted portable electronic devices containing ePHI are stolen.

7) Failure to Adhere to the Minimum Necessary Standard

Covered entities must take steps to limit access to PHI to the minimum necessary information to achieve the intended purpose.

8) Failure to Provide Patients with Copies of PHI on Request

The Privacy Rule permits patients to access PHI and obtain copies of their protected health information on request. Requests for copies of PHI must be dealt with promptly and copies provided within 30 days of the request being received.

9) Failure to Enter into A Business Associate Agreement

Healthcare organizations may require individuals or entities to provide services that require access to PHI. Prior to any disclosure of PHI, the entity that performs those functions must enter into a business associate agreement (BAA) with the covered entity. The BAA outlines the

business associate's responsibilities to safeguard PHI, explains the permissible uses and disclosures of PHI, and other requirements of HIPAA.

10) Failure to Issue Breach Notifications Promptly

In the event of a data breach, notifications must be issued to affected individuals to alert them to the exposure of their PHI. Breach notifications must be issued without unreasonable delay and no later than 60 days from the date of discovery of the breach

Special Warnings In Regard To SOCIAL MEDIA

Facebook, Instagram, Twitter, Linked In and other social media platforms are VERY dangerous for accidentally disclosing PHI. If you respond to a Yelp post by saying, "Thank you", that is a HIPAA violation because you have told the world that person is your patient. They have the patient's name AND that they have a health condition that requires treatment by a Chiropractor. (PHI + Personal Identifiers.)

If you post something and delete it (after realizing it might be disclosing PHI or giving an identifier), remember it is not really deleted from cyperspace. It stays there FOREVER so be very careful about what you post. Think before you post anything related to your practice or any patient.

Patient testimonials require that you get written authorization from the patient before posting it anywhere (your web site, Yelp, etc.)

Finally: Ignorance or Accidents are NO EXCUSE to OCR

The enforcement division (OCR) does not care that you accidentally left a document containing PHI (*both* medical data *and* a Personal Identifier) on a desk in clear view of anyone passing by. It does not care that one of your staff's computer monitor can be seen by a patient standing at the front desk. It does not care that your computer screen in one of your treatment rooms was accidently left on with the last patient's chart on the screen when the next patient is put into that room.

OCR will enforce any and all violations, even accidental disclosures. OCR will enforce any violation that you make even if you do not know about HIPAA. It is a good thing you are taking this course because ignorance is not an excuse when you break the law. "Wow, officer. I didn't know it was against the law to shoot that guy." Ignorance of the law will not help you.

I hope this course has given you a few ideas that you can implement in your practice.

APPENDIX A

APPENDIX A WILL NOT BE TESTED AS PART OF THIS COURSE. I have included it (as an appendix only) to give you a starting point in making a Business Associate Agreement that you can use in your practice and have your "Business Associates" like outside billing companies, collection agencies, etc. sign so that you are HIPAA compliant. You will need to customize it by changing everything in parentheses to something specific for your office or, it may be optional and not apply to your office and then you can take it out.

Business Associate Agreement

This agreement is between (Name of your chiropractic practice) and (Name of BA).

Definitions

Catch-all definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

(b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

[The parties may wish to add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the covered entity.]

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

(e) Make available protected health information in a designated record set to the [Choose either "covered entity" or "individual or the individual's designee"] as necessary to satisfy covered entity's obligations under 45 CFR 164.524;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for access that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to provide the requested access or whether the business associate will forward the individual's request to the covered entity to fulfill) and the timeframe for the business associate to provide the information to the covered entity.]

(f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for amendment that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to act on the request for amendment or whether the business associate will forward the individual's request to the covered entity) and the timeframe for the business associate to incorporate any amendments to the information in the designated record set.]

(g) Maintain and make available the information required to provide an accounting of disclosures to the [Choose either "covered entity" or "individual"] as necessary to satisfy covered entity's obligations under 45 CFR 164.528;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for an accounting of disclosures that the business associate receives directly from the individual (such as whether and in what time and manner the business associate is to provide the accounting of disclosures to the individual or whether the business

associate will forward the request to the covered entity) and the timeframe for the business associate to provide information to the covered entity.]

(h) To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures by Business Associate

(a) Business associate may only use or disclose protected health information

[Option 1 – Provide a specific list of permissible purposes.]

[Option 2 – Reference an underlying service agreement, such as "as necessary to perform the services set forth in Service Agreement."]

[In addition to other permissible purposes, the parties should specify whether the business associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the business associate will de-identify the information and the permitted uses and disclosures by the business associate of the de-identified information.]

(b) Business associate may use or disclose protected health information as required by law.

(c) Business associate agrees to make uses and disclosures and requests for protected health information

[Option 1] consistent with covered entity's minimum necessary policies and procedures.

[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the covered entity's minimum necessary policies and procedures.]

(d) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity [if the Agreement permits the business associate to use or disclose protected health information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add ", except for the specific uses and disclosures set forth below."]

(e) [Optional] Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.

(f) [Optional] Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law, or business associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(g) [Optional] Business associate may provide data aggregation services relating to the health care operations of the covered entity.

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

(a) [Optional] Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate's use or disclosure of protected health information.

(b) [Optional] Covered entity shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate's use or disclosure of protected health information.

(c) [Optional] Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 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

[Optional] Covered entity shall not request business associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity. [Include an exception if the business associate will use or disclose protected health information for, and the agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the business associate.]

Term and Termination

(a) Term. The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement [and business associate has not cured the breach or ended the violation within

the time specified by covered entity]. [Bracketed language may be added if the covered entity wishes to provide the business associate with an opportunity to cure a violation or breach of the contract before termination for cause.]

(c) Obligations of Business Associate Upon Termination.

[Option 1 – if the business associate is to return or destroy all protected health information upon termination of the agreement]

Upon termination of this Agreement for any reason, business associate shall return to covered entity [or, if agreed to by covered entity, destroy] all protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, that the business associate still maintains in any form. Business associate shall retain no copies of the protected health information.

[Option 2—if the agreement authorizes the business associate to use or disclose protected health information for its own management and administration or to carry out its legal responsibilities and the business associate needs to retain protected health information for such purposes after termination of the agreement]

Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

1.
    1. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;
    2. Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;
    3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;
    4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate"] which applied prior to termination; and
    5. Return to covered entity [or, if agreed to by covered entity, destroy] the protected health information retained by business associate when it is no longer needed by business associate for its proper management and administration or to carry out its legal responsibilities.

[The agreement also could provide that the business associate will transmit the protected health information to another business associate of the covered entity at termination, and/or could add terms regarding a business associate's obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors.]

(d) Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.

Miscellaneous [Optional]

(a) [Optional] Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) [Optional] Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) [Optional] Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

_____ _____

Signature of Business Associate Authorized Representative Date Signed

_____

Written Name of Business Associate Representative