

ExecTech Guideline

Five Steps to HIPAA Privacy Rule Compliance

HIPAA, the Health Insurance Portability and Accountability Act, became law in 1996. Its original intent was to help employees change jobs and keep their health insurance by making their coverage “portable.” Lawmakers broadened the law to include the Privacy Rule which went into effect on April 14, 2003.

Why Do We Need Privacy Laws?

The following examples help explain why the US Government created the HIPAA Privacy Rule.

- St. Elizabeth's Medical Center is being sued by an Illinois woman for releasing her medical records and her photograph to anti-abortionists. They posted details of her abortion procedure complications on the Internet.
- An insurance company released an Atlanta truck driver's medical records to the trucking company. The driver was fired when the company learned he had been seeking treatment for a drinking problem.
- A health worker in Tampa sent the names of 4,000 people with positive HIV test results to two newspapers.
- Eli Lilly mailed free Prozac samples to Florida patient lists obtained from Walgreens.
- The 13-year-old daughter of a hospital worker took a list of patients' names and phone numbers. As a joke, she called the patients and told them they were diagnosed with HIV.
- Country singer Tammy Wynette's medical records were sold to the National Enquirer by a hospital employee for \$2610.

Who Must Comply with the Privacy Rule

If you are a paper-based practice, meaning you do not transmit any patient information electronically, compliance to the Privacy Rule is voluntary. However, for the majority of practices, the speed, accuracy and cost savings of electronic billing vital to success.

Electronic transmission includes sending Protected Health Information (PHI) over the Internet, with any kind of digital storage system, or with email. Fax transmissions are not included in the definition.

Go to www.cms.gov/HIPAAgenInfo/04_PrivacyandSecurityStandards.asp for details about who must comply with the Privacy Rule.

What is Protected Health Information (PHI)?

Protected Health Information (PHI) is a HIPAA term that is used throughout this guideline. PHI includes all medical records and health information of an individual.

A patient's health information is protected in any form: paper, electronic, oral. You may control PHI in many forms: backup computer disks or tapes, insurance statements, prescription forms, lab reports, correspondence from other doctors, patient forms, email, explanation of benefits notices, treatment authorizations, collection documents, conversations between doctors and staff, faxes regarding patients and so on.

Five Steps to Privacy Rule Compliance

1. Put someone in charge.
2. Keep Protected Health Information (PHI) secure and private.
3. Set up office policy, implementation procedures and training for your staff.
4. Inform patients of their rights and support those rights.
5. Limit access of patient information to businesses outside the practice.

1. Put Someone in Charge

The Privacy Rule requires you to assign responsibility to someone to implement the Privacy Rule. The Privacy Officer's job is to get the other four steps in this guideline done and keep them in place.

In small practices, this can be the doctor or office manager. In large practices, it may be a full-time job for a few weeks and a part-time job thereafter.

Privacy Officer Duties

- Keep track of the steps you take to comply with the HIPAA Privacy Rule. For example, record the date you install a door lock to your file room.
- Take any steps needed to keep all PHI under your control private and secure.
- Create and update a Privacy Notice for your patients, a privacy policy for the staff, staff training material and other paperwork.
- Ensure current and new staff are trained on the HIPAA Privacy Rule as it applies to your practice.
- Enforce the practice's privacy policy.
- Arrange for all patients to receive and sign the Privacy Notice acknowledgment form.
- Help individuals who wish to see and review their files, receive copies of their files, request changes to their PHI or other requests or questions.
- Keep records of Privacy Rule activities including who has been trained and when, who has keys or combination codes, patients and outside parties who have requested PHI, patient complaints, patient requests and so on.
- Store all forms and records related to the Privacy Rule for at least six years. Ask the Practice Owner for approval of your filing system. For example, will you keep the Privacy Rule paperwork in patient files, in separate Privacy Rule files or both.
- Plug any PHI leaks as they come up.
- Learn and implement state privacy rules that apply to the practice.

2. Keep Protected Health Information (PHI) Secure and Private.

You probably keep PHI private and secure already, so being in compliance will not be difficult. To comply with this part of the Privacy Rule, simply accept responsibility and use your judgement for keeping all PHI secure and private.

The law does not require you to replace your file cabinets or build new walls. It says to take "reasonable" efforts to prevent unauthorized access to PHI.

For example, perhaps you can change the file room door knob without a lock, to a door knob with a lock. Many file cabinets have a metal piece at the top you can punch out to install a lock. You may decide you only need to hang a sign that says, "Authorized Personnel Only."

When employees stop working for the practice, you don't need to replace or re-key your locks to protect PHI, unless that is your normal routine. Many practices simply change the burglar alarm code. Another good idea is to install door locks that you open with a combination code instead of a key.

The Privacy Officer should look through the practice, list all the potential PHI leaks and get them plugged. He or she should make a list of all changes made to prove, if needed some day, that the practice made reasonable efforts to comply.

Examples:

Computers

- Give all computer users their own computer password.
- Set up your software to limit access to PHI to those who need it to do their jobs.
- Keep computer backup copies secured or locked up.
- Position computer screens so people passing by cannot read any PHI.
- Set up screen savers that blank out the screen when not in use for a few minutes and require passwords to open again.

- If you send or receive PHI through email, you need to encrypt the messages. An email system like relayhealth.com may fit your needs. See ExecTech article, "Seventeen Benefits of Using Email with Patients" (www.exectechweb.com/email.htm).
- When an employee leaves, cancel their computer password and get their keys.

Files and Papers

- Keep patient files and charts locked up when not in use.
- Shred paper with PHI. Do not throw it away or recycle it. Use a cross-cut shredder, not a strip-cut shredder as strips can be scanned and reassembled by a computer software. If you have a large quantity of material to shred, you can hire a document destruction company.
- Ensure the patient sign up sheet does not ask for "reason for visit."
- If you use clear chart holders on doors, tape a piece of paper in the holder so patient charts cannot be read by people walking by.
- Remove or hide patient schedules, progress charts, surgery schedules or other PHI where the public or patients can see them.
- Publish patient names in your newsletter or promotional material only with their written consent.
- Don't leave documents, faxes or reports with PHI on desks or counters when not in use. Put them in folders or turn them over so they cannot be read.

Communications

- Lower your voice when discussing PHI with patients, doctors or staff where other patients can overhear you.
- Check your waiting areas to ensure patients cannot overhear telephone conversations.
- When leaving messages for patients on a machine or with a person, keep the message brief and use good judgement. For example, an abortion clinic or drug-rehab facility should be very discreet while a dentist or chiropractor has less to worry about.
- Send reminder postcards with good judgement, as well. Even an envelope from certain types of practices can make patients feel their privacy is at risk.
- When in doubt, ask the patient what he or she wants. "When we get your lab results, how should we contact you?"
- When calling out names to waiting patients, do not also mention their service. You can say, "Bob Jones? Come this way." Do not say, "Bob Jones? Ready for your chemo?"

Minimum Necessary Uses and Disclosures

As well as protecting PHI, you need to release or provide access to PHI when required.

You do not block PHI access to the patient, anyone authorized by the patient, anyone who needs the data for treatment purposes, or uses/disclosures required by law.

Use your judgement on how much to allow. For example, a temporary receptionist does not need access to patient records, but does need access to scheduling information. An insurance company request for information may only require a progress report and not the entire file.

3. Set up Office Policy, Procedures and Training for Your Staff

The Privacy Officer needs to train the current staff and future staff on the Privacy Rule. "Staff" includes doctors, partners, associates, spouses, part-time and full-time employees, independent contractors and anyone else who works in the office. New employees must be trained within a reasonable amount of time. Business associates are not included (see Step 5).

Written guidelines are the easiest and best way to train people. So the first step is to tailor the rules to your practice. See Attachment 1 "How to Write Your Office Privacy Policy."

Create a checklist of all the written material required to be read as part of the training. Attach this material as part of the office policy. You can require all staff to read this guideline and its attachments as part of your training process.

Hold a staff meeting to go over the written material. Have everyone sign a form stating they understand the material and will enforce the office policy.

During the training sessions, go over all forms of PHI in the practice and how it must be kept private and secure. Explain the patient's rights and how the practice will support those rights.
Ensure everyone understands the law and has no confusion or unanswered questions.
Additional training material is available from the links at the end of this guideline.

4. Inform Patients of their Rights and Support those Rights

You need to inform your patients of their privacy rights under the HIPAA Privacy Rule. This includes their right to see their PHI, to change or amend their PHI, and to get assistance to their privacy complaints.

“Notice of Privacy Practices” Wording

Except for the first paragraph in Attachment #2 “Sample Notice of Privacy Practices,” you can use any wording you like to explain the patients' rights as long as it is written in plain language.

The notice should include the patient's rights under the HIPAA Privacy Rule, how to file a complaint, the name and number of the Privacy Officer, when the rule goes into effect, the practice's right to change the notice, the right of patients to request tighter restrictions to their privacy and so on. Details about the notice can be found in section 164.520(b) of “Standards for Privacy of Individually Identifiable Health Information” (the HIPAA Privacy Rule). See: www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

Privacy Notice and Acknowledgment

The HIPAA Privacy Rule requires you to give the patient a “Notice of Privacy Practices.” See Attachment #2 “Sample Notice of Privacy Practices.” Tailor a notice to fit your practice and your needs.

You give each patient a copy at his or her next appointment and ask him or her to sign the acknowledgment. The patient can have a copy if he or she wants one.

If the patient is a minor or represented by a guardian, have the parent/guardian sign for the patient. This same person can also act for the patient in obtaining copies of the patient's PHI, submitting changes for the file, or filing a complaint on the patient's behalf.

In an emergency situation, the notice can wait until the emergency is over.

Each new patient will also need to sign the acknowledgment at their first visit.

Once the patient has signed the acknowledgment, file the form.

The law requires you to make “reasonable efforts” to do this step. If you cannot get a patient to sign the acknowledgment, write down what happened and file it as you do the other forms.

As well as handing the notice to patients, the law requires you to post the notice in a prominent location, such as on the wall in your reception area. We suggest you frame it with glass so it continues to look professional through the years.

If your office gives services through email, send the patients the notice just before giving the next email service. Ask the patient to acknowledge receiving the notice via email. He or she may also have a paper copy, if requested.

Finally, the Privacy Rule states that if you have a website, you need to post your privacy notice there.

Consent

If you wish to share a patient's information to an outside company, such as a marketing list company, you need written consent from each patient.

Marketing your own services or products directly to your patients, or giving samples or literature yourself, is not a violation of the Privacy Rule.

Extra Privacy Restrictions

As described in the patients' Privacy Notice, any patient may request additional privacy restrictions. For example, he or she may request that only a certain doctor may read the PHI.

Ask the patient to submit the request for extra privacy in writing. The Privacy Officer reviews the request, makes a recommendation and submits the request to the Practice Owner for approval or denial.

You (the doctor) are not required to approve these requests, but you must consider them. If you agree to an extra privacy restriction, you must keep your word.

Keep the related paperwork on file.

Confidential Communications

The Privacy Notice states the patient may receive communication from your office in a specific way. For example, he or she may not want you to call him or her at work. The HIPAA Privacy Rule requires you to follow these instructions if at all possible.

If the request is difficult, you can refuse. For example, the patient wants his statement sent via email and only on Wednesday evenings. Instead, offer a solution that is not a difficulty for the practice. For example, have the patient prepay the copayment so no statement is necessary. Or suggest he ask for a copy at his next visit.

Never ask the patient to explain why he or she has the request.

If the request is reasonable, you must do it.

Releasing PHI to the patient

Patients have the right to see their PHI upon request within 30 days. If you need more time, you can extend the deadline by 30 days if you provide the individual with a written statement of the reasons for the delay. However, a well-organized practice can fulfill such requests quickly.

State laws may have stricter rules which will override the federal law. Examples:

California law gives you five days to show the PHI and 15 days to provide copies.

Florida law says to provide the patient his or her information “in a timely manner, without delays for legal review.”

Colorado law says you must provide access or copies within a “reasonable amount of time.”

Maryland law says, “The provider must respond within a reasonable time, but no more than 21 days after receipt of the request.”

Virginia law gives you 15 days.

Have the patient write down his or her request to see the PHI or obtain copies of PHI. Ask the patient to note if he or she wants anything in particular, such as financial records, or all the PHI you have. Create a form for your practice, if you wish.

The Privacy Officer should record all requests to access or receive copies of PHI. He or she should then send you (the doctor) the request and the patient’s file for a decision.

According to HIPAA law, you (the doctor) may deny access to some or all of an individual’s PHI if it contains psychotherapy notes, if the information will be used in a lawsuit or government action, if you received the information under a promise of confidentiality and releasing it would reveal the source, and other legal reasons. When in doubt, check the Privacy Rule laws available through the web site at the end of this guideline. Or get an attorney’s assistance.

You may also deny access if you (the doctor) feel that releasing PHI might endanger the individual or another person (e.g., releasing child abuse information to the potential abuser). In this case, the individual may request a review of your denial.

If the individual requests a review, you designate a licensed healthcare professional who is not involved in your decision, as the reviewer. He or she reviews the PHI and your denial and provides the individual with a written notice of his or her decision.

Under the Privacy Rule, if you deny a request, you must provide a written explanation. You must also include the details about a review you have arranged and instructions on how to file a complaint to you or the Department of Health and Human Services.

If the request is approved, you may charge a reasonable fee. However, if requests are infrequent, you may wish to help the patient at no charge as a goodwill gesture. Check your state’s law for any guidance on fees.

Of course, make sure the person you are giving access to or copies of PHI is the right person (check ID if you don’t know him or her personally).

Keep all paperwork secure in case you need to prove in the future you followed the rules.

Amendments

Patients can ask you to change some aspect of their PHI. For example, he or she disagrees with your diagnosis regarding a pre-existing condition.

Per the Privacy Rule, you have 60 days to respond to an amendment request, but for best service, you should respond within a week.

If you approve or disapprove the patient's request, let him or her know. Either way, explain your decision. Tell the individual he or she has the right to submit a statement for the file or that their request can be included in the file. Also explain how he or she can file a complaint with the Department of Human Services.

If you do not have the PHI the patient wants changed, let him or her know this and where the PHI is located.

Keep the paperwork on file.

Complaints

If a patient complains about your privacy practices to the Department of Human Services, you may be investigated. So you want the patient or guardian to feel comfortable giving you their complaint so you can resolve the problem.

Ask the patient to put the complaint in writing. Investigate the problem. Write a letter to the patient explaining what you did to resolve the problem. Attach quotes from the law if the patient is actually complaining about your compliance to the law. Then meet with the patient, go over the letter and make sure he or she is happy.

Fully resolve any privacy weaknesses or errors with better staff training or new procedures so the problem never repeats.

As with all privacy paperwork, keep it on file.

5. Limit Access of Patient Information to Businesses Outside the Practice

So the rule is: don't sell your patient information to outside companies without the patients' consent. Since you probably never have nor will sell patient information, compliance with this rule is easy.

Other types of businesses and individuals may have access to your patient records if they sign an agreement. For example, you might hire a consultant who looks at patient files to evaluate your patient management strengths and weaknesses. The consultant needs to sign an agreement with you that protects the privacy of the patient information. See Attachment #3 "Business Associate Protected Health Information Agreement"

Businesses and individuals who come to your office as part of normal business do not need to sign an agreement. For example, people who clean, repair or maintain your facility or equipment.

The HIPAA Privacy and Security Rules state that you need an emergency data backup and recovery system. An online backup system is perfect for this requirement. Online backup companies use sufficient security measures as part of their service and so per the law, you do not need a business associate agreement with the backup company.

Examples of organizations, that deal with PHI, with which you need business associate agreements.

Telephone answering services

Billing companies

Consultants

Accountants and bookkeepers

Attorneys

Collection agencies

Software companies

Computer technicians

Transcription services

Quality insurance/credentialing services

Malpractice carriers

Document destruction firms

Research agencies

Schools

The following are usually not business associates as they do not deal with PHI even though they may be in your office:

Janitors
Maintenance or construction workers
Couriers
Equipment technicians
Patient finance firms

These individuals and groups are not normally classified as business associates as they are part of routine treatment and payment procedures:

Other healthcare providers and staff
Home care providers
Hospitals
Labs
Imaging centers
Pharmacies
Managed care plans
Insurance companies that cover your patients' services
Government agencies
Someone who is required by law to perform a function
Employees, associates or others who receive your privacy law training

Your written agreement with Business Associates must state he or she will safeguard the PHI and not use or disclose the information beyond the terms of the contract or by law. The agreement can be part of a larger agreement with the Business Associate, or a separate agreement.

You do not need to monitor your Business Associates use of the PHI you provide. However, if there is a complaint or problem with the Business Associate, you must deal with it.

See Attachment #3 "Business Associate Protected Health Information Agreement" for a sample wording for occasional PHI use by the Business Associate whose purpose is to assist the practice (e.g., management consultant, software technician, etc.). If the relationship involves complex activities with your files or significant involvement with PHI, get an attorney to assist you with the contract. The Department of Health and Human Services has created and posted sample wordings for a Business Associate contract at www.hhs.gov/ocr/privacy/hipaa/understanding/coveridentities/contractprov.html

Additional Information

If the Department of Health and Human Services contacts you or wants to give you a compliance review, hire an attorney that specializes in healthcare privacy law.

Before dealing with a complicated request from a patient, make sure you know what you are doing. You might save a lot of time and money if you read the law or related document before calling an attorney. Fortunately, the Internet has a wealth of valuable information on the HIPAA Privacy Rule.

While there are dozens of useful web sites, books and workshops, the US Government web site is the most useful: www.hhs.gov/ocr/privacy

Good luck!

Attachments

- #1: "How to Write Your Office Privacy Policy"
- #2: "Sample Notice of Privacy Practices"
- #3: "Business Associate Protected Health Information Agreement"

Attachment #1: How to Write Your Office Privacy Policy

The sample policy below must be modified to fit your practice. For example, add your practice name and the name of your Privacy Officer. Write out your specific security procedures (who locks what and when) and include it in this policy or in an attachment.

Keep the policy simple and easy to understand. Attach anything else you wish the staff to learn as part of their training.

The practice owner or CEO must review and approve the final policy wording.

Have all staff members sign the policy as part of their training.

Office Policy on Privacy (Sample)

Protecting our patients' privacy is important to this practice. We also wish to make every effort to comply with state and federal privacy laws.

Rules:

1. We are responsible for keeping our patients' Protected Health Information (PHI) confidential.

PHI includes all medical records and health information of an individual. PHI is in many forms: paper, electronic, oral and includes our computer files, paper files, computer disks or tapes, insurance statements, prescription forms, lab reports, correspondence from other doctors, patient forms, email, explanation of benefits notices, treatment authorizations, collection documents, conversations between doctors and staff, faxes regarding patients and so on.

2. Our practice has a Privacy Officer who makes sure we comply with the privacy laws. See him or her for any questions regarding patient information privacy. Send all information, questions and paperwork related to this policy to the Privacy Officer including patient forms, complaints, requests for file changes, questions, violation reports, contracts and requests for or access to PHI.

3. All staff, including doctors, part-time staff and others who work here must be trained in the HIPAA (Health Insurance Portability and Accountability Act) Privacy Rule. Reading this policy is part of that training. You will be asked to sign a form stating you have read and understand your role in maintaining our patients' privacy.

4. All current patients and all future new patients will be given a copy of "Notice of Privacy Practices" that explains their rights according to the HIPAA (Health Insurance Portability and Accountability Act) Privacy Rule. We will ask each patient to sign the notice showing they received the notice and keep the form on file. Each patient may have a copy of the notice.

This Privacy Notice is attached. Please read it to ensure you understand and will support our patients' rights.

4. PHI is available to those in the practice who need it to do their jobs. The Privacy Rule does not restrict its use in treatment, payment or routine healthcare operations. For example, when we refer a patient to another doctor, he or she can have as much access to PHI as he or she needs or wants.

However, if you or others do not need access to PHI to do your job, your access is restricted.

5. When we release PHI to non-healthcare people, we will only release the PHI that is needed for their purpose and only after the Privacy Officer and doctor approve the release.

For example, if a patient wants a copy of his last five billing statements, that is all we provide. We do not give him a copy of his entire file unless he asks for it and even then, we may not give him everything as state and federal laws want the doctor to use judgement in giving PHI to patients (e.g., information that may harm the patient or someone else).

As another example, if a life insurance company has signed permission from a patient to release his or her exam results, we only give the exam results.

So when asked for PHI, simply get the request in writing and promise to pass it on to the Privacy Officer.

6. Except for ourselves, we do not allow anyone to use our patient lists or information for marketing purposes.

7. Outside firms and workers, who do not work here, may have access to PHI if they sign a Business Associate contract. For example, a software technician or consultant may look at PHI as long as he or she has signed the contract.

8. Do your part to keep PHI private and secure. For example, follow all the procedures for security and privacy the Privacy Officer gives you. Never throw away or recycle anything that contains PHI; use the shredder. If you discuss cases outside the office, do not include anything that can identify the person, such as the individual's name.

9. Any violations of the Privacy Rule, the state privacy laws or this policy must be corrected. All violators will have reports of the violation filed in their personnel files. Repeat violations may result in a suspension or termination.

10. If you see or know of a violation of this policy or the privacy laws, please report it to the Privacy Officer, preferably in writing. By law, you cannot be punished for reporting a violation.

11. This practice can be fined and violators can be jailed for violations of this law.

For example, if one of our staff members secretly made a copy of our overweight patient's names and mailed a letter to these patients to sell a weight-loss product, that person could be fined and jailed by the government and then sued by the patients. The practice could also be penalized for hiring and trusting such a dishonest person.

On the other hand, the lawmakers understand slips and mistakes are inevitable. For example, you accidentally mention a patient's name and condition to the wrong person. Just be sure to take steps to prevent similar mistakes in the future.

Attachments

1. "Notice of Privacy Practices"
2. ExecTech Guideline, "Five Steps to HIPAA Privacy Rule Compliance"

Written by _____

Approved by _____

Employee Acknowledgment

I _____ have read and understand the Office Policy on Privacy and its attachments. I will comply with and help enforce each part of the policy.

Signed _____

Date _____

Attachment #2: ABC Clinic Notice of Privacy Practices (Sample)

This notice describes how your health information may be used and disclosed and how you can access this information. Please review it carefully.

At ABC Clinic, we have always kept your health information secure and confidential. A new law requires us to continue maintaining your privacy, to give you this notice and to follow the terms of this notice.

The law permits us to use or disclose your health information to those involved in your treatment. For example, a review of your file by a specialist doctor whom we may involve in your care.

We may use or disclose your health information for payment of your services. For example, we may send a report of your progress to your insurance company.

We may use or disclose your health information for our normal healthcare operations. For example, one of our staff will enter your information into our computer.

We may share your medical information with our business associates, such as a billing service. We have a written contract with each business associate that requires them to protect your privacy.

We may use your information to contact you. For example, we may send newsletters or other information. We may also want to call and remind you about your appointments. If you are not home, we may leave this information on your answering machine or with the person who answers the telephone.

In an emergency, we may disclose your health information to a family member or another person responsible for your care.

We may release some or all of your health information when required by law.

If this practice is sold, your information will become the property of the new owner.

Except as described above, this practice will not use or disclose your health information without your prior written authorization.

You may request in writing that we not use or disclose your health information as described above. We will let you know if we can fulfill your request.

You have the right to know of any uses or disclosures we make with your health information beyond the above normal uses.

As we will need to contact you from time to time, we will use whatever address or telephone number you prefer.

You have the right to transfer copies of your health information to another practice. We will mail your files for you.

You have the right to see and receive a copy your health information, with a few exceptions. Give us a written request regarding the information you want to see. If you also want a copy of your records, we may charge you a reasonable fee for the copies.

You have the right to request an amendment or change to your health information. Give us your request to make changes in writing. If you wish to include a statement in your file, please give it to us in writing. We may or may not make the changes you request, but will be happy to include your statement in your file. If we agree to an amendment or change, we will not remove nor alter earlier documents, but will add new information.

You have the right to receive a copy of this notice.

If we change any of the details of this notice, we will notify you of the changes in writing.

You may file a complaint with the Department of Health and Human Services, 200 Independence Avenue, S.W., Room 509F, Washington, DC 20201. You will not be retaliated against for filing a complaint.

However, before filing a complaint, or for more information or assistance regarding your health information privacy, please contact our Privacy Officer, Jill Jones, at (123) 456-7890.

This notice goes into effect as of April 14, 2003.

Acknowledgment

I have received a copy of the ABC Clinic Notice of Privacy Practices.

Date _____

Signed _____ Print Name _____

If signing as a parent or guardian, please note the name of the patient _____

Attachment #3: Business Associate Protected Health Information Agreement

This Agreement, made on the _____ day of _____, 20____, is by and between

_____ (referred to as “The Healthcare Practice”) and

_____ (referred to as “Business Associate”).

The Healthcare Practice has the responsibility for safeguarding Protected Health Information (referred to as “PHI”) of its patients. PHI includes all medical records and health information of an individual in any form including paper, electronic and oral.

Business Associate agrees to not use or disclose PHI other than as permitted or required by this Agreement or as required by law.

Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the PHI beyond the terms of this Agreement.

Business Associate agrees to report to The Healthcare Practice any use or disclosure of the PHI not covered by this Agreement of which the Business Associate becomes aware.

Business Associate agrees to ensure that any agent, representative or employee of Business Associate, including a subcontractor, to whom it provides PHI from The Healthcare Practice, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate.

Business Associate agrees to make PHI and related records obtained from The Healthcare Practice available to The Healthcare Practice and the Department of Health and Human Services to determine The Healthcare Practice’s compliance with the Privacy Rule.

The Healthcare Practice agrees to disclose PHI to Business Associate the minimum amount of PHI necessary for the Business Associate’s purposes.

Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of The Healthcare Practice, provided that such use or disclosure does not violate the Privacy Rule.

If Business Associate violates the terms of this Agreement, The Healthcare Office will make reasonable attempts to resolve the violations. If a resolution is not feasible, The Healthcare Office will report the violation to the Department of Health and Human Services.

Either party may terminate this Agreement at any time without reason or notice.

Upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received from The Healthcare Practice. Business Associate shall retain no copies of the PHI.

The rights and obligations of Business Associate of this Agreement shall survive the termination of this Agreement.

Any ambiguity in this Agreement shall be resolved to permit The Healthcare Practice to comply with the Privacy Rule.

This Agreement goes into effect as of the _____ day of _____, 20_____.

Signed:

The Healthcare Practice

Business Associate

Date

Date