**ExecTech Guideline**

**Six Steps to HIPAA Rules 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.

ExecTech’s original guideline, “Five Steps to HIPAA Privacy Rule Compliance” came out in March 2003. The law was relatively simple to understand and comply with. No one was getting fined or investigated.

However, the law has become more complicated than ever, and the audits, investigations and fines have skyrocketed. The Health and Human Services Office for Civil Rights (called the HSS in this guideline) has become a powerful government agency that is collecting millions in fines each year. All health-care providers need to comply with the HIPAA law.

Even though we are updating this guideline in 2016, it does not cover every possible aspect of the law. It is, however, an excellent starting point for understanding and complying with the law, especially if you are new to the world of HIPAA.

**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 was 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.

**Examples of HIPAA Privacy Rule Violations**

Cancer Care Group, an Indiana radiation oncology group with 13 doctors, agreed to pay $750,000 for its HIPAA violations. A laptop, stolen from an employee’s car, contained the Protected Health Information (PHI) of approximately 55,000 Cancer Care patients. Prior to the breach, Cancer Care was in major non-compliance with the HIPAA Security Rule. As well as paying the $750,000, Cancer Care has taken top-priority action to comply with the HIPAA Privacy Rule.

An unencrypted thumb drive, with the PHI of 2,200 patients was stolen from a vehicle of the staff member of the Adult & Pediatric Dermatology (APDerm) of Concord, Mass. APDerm did not have policies and procedures in place to address the breach. The investigation revealed that APDerm had...
not conducted an assessment of the potential risks to the confidentiality of PHI as part of its security management process. APDerm agreed to pay $150,000 as well as implement a corrective action plan.

The laptop of an QCA Health Plan, Inc.’s staff member was stolen. The laptop had ePHI of just 148 individuals in it. QCA agreed to a $250,000 settlement and several other actions to meet HIPAA requirements.

Dental Practice Investigations

Most of the completed investigations and fines have involved hospitals, health plans, pharmacies, medical practices and mental health practices. While the HSS does not show cases that are in the works, there are two public cases involving dentists:

1. A patient filed a complaint that a dental practice had a red sticker with the word “AIDS” on the outside cover of his chart. Other patients could read the sticker. When notified of the complaint, the dental practice immediately removed the red AIDS sticker from the patient’s file. To resolve this matter, the HSS also required the practice to revise its policies and operating procedures and to move medical alert stickers to the inside cover of the records. Further, the dental practices Privacy Officer and other representatives met with the patient and apologized, and followed the meeting with a written apology.

2. Burglars broke into a Rocklin, CA dentist’s office and stole everything that wasn't bolted down, including his main unencrypted computer. To comply with the law, he notified his patients, the media, the State of California and the HSS. While he waits for his investigation, he is quite stressed. You can read the details here: www.cda.org/news-events/burglary-leads-to-lengthy-hipaa-investigation-for-cda-dentist

Who Must Comply with the HIPAA Rules

All healthcare practitioners, health plans and healthcare clearinghouses.

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. When the information is digital, the government calls it ePHI, but we just use PHI in this guideline.

A patient’s health information, in any form, is protected: paper, electronic, even oral. More specifically, you have PHI in your computer backup data, 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.

Six 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.
6. Conduct a Risk Assessment to test your security.

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 and keep your practice in compliance with HIPAA rules.

In small practices, this can be the practice owner, spouse or responsible staff member. 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.
- Securely store all forms and records related to the Privacy Rule for at least six years. If the practice is ever audited or investigated, you will need to provide all related paperwork.
- 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.

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 and Devices
- Make a list of every location of PHI. Such as your main computer, your backup disks, thumb drives, mobile devices, paper files and so on. Write a plan that will protect all of the information at each location.
- Give all computer users their own computer passwords.
- Consider encrypting all PHI. See www.exectechweb.com/protect for more information.
- Set up your software to limit access to PHI to those who need it to do their jobs.
- Take steps to prevent computer viruses and ransomware infections by you or your staff. See www.exectechweb.com/ransomware for eight recommendations.
- Keep computer backup copies secured online or physically locked up.
- Consider moving your entire practice-management system online (onto the cloud) and let your system’s people worry about it.
- 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.
- The Privacy Rule allows you to communicate with your patients by email as long as you use reasonable safeguards. For example, you need to make sure you are using the email address your
patient wishes you to use to send private health information. If you get a confirmation email reply from
the patient first, you are taking reasonable safeguards. Of course, if a patient starts the email
communication with you, no additional precautions are necessary. To ensure email is still allowed, go to:
www.hhs.gov/hipaa/for-professionals/faq/570/does-hipaa-permit-health-care-providers-to-use-email-to-
discuss-health-issues-with-patients
☑ When an employee leaves, close off their ability to use your computer and get his or her keys.
☑ Protect the information on all your mobile devices with encryption. If the device is lost or stolen, you
will still be in compliance with the HIPAA Privacy and Security Rules.

Review Websites
☑ We encourage you to post responses to patient reviews in certain circumstances (see ExecTech’s
book, “Yelp Help for Healthcare Providers”). However, do not post anything about the patient’s
symptoms, diagnosis, procedure, dates of visits or anything related to his or her condition on the
internet, even if the patient brings it up first. Just because the patient brings it up, or even if the
patient’s last name is not included in the review, the Privacy Rule still applies. You need the patient’s
written permission to include his or her PHI in your public review comments with Yelp, Angie’s List,
Google+ and so on.

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, hire a HIPAA-compliant 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?”
☑ When individuals privately pay for their visits, they can instruct you to not to share information about
their treatment with their health plan. Comply with their instructions.

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 with their privacy concerns.

Find or Create Your “Notice of Privacy Practices” Wording

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.

You can use the Privacy Notice provided by your state or US association, such as the American Dental Association. You can also use a notice provided by the HSS.


Just customize the notice to include your practice name and your type of practice.

Make sure you understand all the words, sentences and paragraphs of your notice in case you need to explain it to a patient.

Give the Privacy Notice to Patients and Get an Acknowledgment

The HIPAA Privacy Rule requires you to give every patient a copy of your “Notice of Privacy Practices.”

You give each patient a copy at his or her first 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.

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 with 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 or receive a copy of their PHI (paper or electronic) within 30 days. You cannot deny the request if the patient owes money to the practice. If you need more than 30 days, 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.

Not Informing Insurance Carriers

If a patient has insurance coverage, but pays for the visit privately, he or she can request that the details of that visit not be revealed to the insurance company. You must comply with this request.

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 complaining to you 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

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 #2 “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.

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
- Employees, associates or others who receive your privacy law training

However, when in doubt, get the person or organization to sign a Business Associate Agreement.

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 #2 “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/coveredentities/contractprov.html](http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html)

### 6. Conduct a Security Risk Assessment

Once you have implemented the steps of this guideline, you now need look for all the ways you might be at risk. This step is not optional.

Medical practices that accept payment from Medicare or Medicaid, are required to conduct a security risk assessment in order to qualify for the “meaningful use” incentive payments ($44,000 over five years for Medicare and $63,750 over five years for Medicaid). Meaningful use means the practice uses electronic health records in a meaningful manner, such as electronic prescribing.

To conduct a risk assessment, you look at dozens of ways you might lose control of your patients’ PHI. For example, could a former staff member get into your patient files? Are all the devices with PHI in them encrypted or under lock and key? Is there an easy way for a hacker to get into your systems?

You can do this assessment by yourself or you can hire a HIPAA security firm to do it for you.

**Do It Yourself**

The HSS has created a HIPAA Security Risk Assessment Tool that you can download at [www.healthit.gov/providers-professionals/security-risk-assessment](http://www.healthit.gov/providers-professionals/security-risk-assessment). On this same website page, you can watch tutorials and read how to use the tool. You then answer 156 difficult-to-understand questions. With each question, you can read additional information about the question. After you get through the questions, the tool then gives you a list of things you need to do.

You can also use checklists that are easier to understand, but time consuming. If you are tech savvy and have a one-doctor practice with little sensitive data (AIDS, drug abuse, cancer, etc.) about your patients, using a risk assessment checklist is fairly easy to do. Your state or national association has checklists you can download.

For example, the American Dental Association’s “ADA Practical Guide to HIPAA Compliance” includes its “Sample HIPAA Security Risk Assessment for a Small Dental Practice” or the American Podiatric Medical Association’s “Risk Assessment Checklist.”

Private security firms also offer risk assessment checklists, including:

- [www.hipaajournal.com/hipaa-compliance-checklist](http://www.hipaajournal.com/hipaa-compliance-checklist)
- [http://hipaanews.org/checklist.htm](http://hipaanews.org/checklist.htm)

However, the HSS writes, "... doing a thorough and professional risk analysis, that will stand up to a compliance review, will require expert knowledge that could be obtained through services of an experienced outside professional."

**Hire a HIPAA Security Firm**

A complete industry of HIPAA security experts has sprung up to help you comply with Step Six. They can remotely examine your computer system, make changes for you and give you a list of recommendations.

The fees vary depending on your profession, the number of your clinics and the services you need. They can help you on an hourly or annual basis. Fortunately, their fees are not very high
If you have not yet worked with one of these firms, ask your colleagues, your groups/societies and Google. For example:
https://hipaariskadvisor.com
www.nguard.com/hipaa-compliance
www.pondurance.com/hipaa-security-services

Below is a response from one of our client’s questions about a security firm’s fees:
“Generally a good rule of thumb is 30-45 minutes per computer and a hour to an hour and a half per server to audit. Not much is required on your part. We can do a great deal of it remotely and off peak business hours so we don't interrupt patient flow. What we do is go through each computer and make sure it meets compliance requirements for HIPAA and HITECH. We also fix any issues we come across that are not compliant or security vulnerabilities. You are on a monthly maintenance contract so the fee is $95 per hour as opposed to $125.00 per hour. When complete, you get a full report, network mapping, password logs, and network diagram. Include our report in your Risk Analysis” (http://bellcurvetechnology.com)

The doctor decided to use this firm instead as it did the same type of work for less:

How to Handle Missing Device Losses or Thefts
How to Handle Missing Device Losses or Thefts
How to Handle Missing Device Losses or Thefts
How to Handle Missing Device Losses or Thefts

As covered in “How to REALLY Protect Your Patients’ ePHI” (www.exectechweb.com/protect), your best option to avoid HIPAA penalties is full encryption. You can do this by either:
1. Moving your practice data and computer functions to an online practice management system.
2. Encrypt all of your devices, including your main office computer and backups. If an encrypted device is lost or stolen, you simply buy a new one, install your software and copy your backup data to the device.
   If you cannot do 1 or 2 above, take strong measures to protect your devices from loss or theft.
   If a device of yours, that contains PHI, is lost or stolen and it is not encrypted, contact your state association’s legal department or hire an attorney who specializes in healthcare privacy law. You must notify the patients and take corrective actions within 60 days.

How to Handle a Cyber Attack
Even if your system is encrypted, a hacker can take control of your data if one of you or one of your employees allows a virus or other bad software to get in. If you lose control of your patients’ PHI, you have a PHI breach. If this occurs, contact your state association’s legal department or hire an attorney who specializes in healthcare privacy law. You must notify the patients and take corrective actions within 60 days.
   However, if you follow the steps in “Ransomware” (www.exectechweb.com/ransomware) the odds of a cyber attack are greatly reduced.
   Of course, if you are using an online practice-management system, you have nothing to worry about. If a hacker somehow gets to your data, it’s the fault of your system’s company, not yours.

Breach Insurance
You can buy or may already have breach insurance. If you lose control of 500 or more patients PHI, you are required by law to notify patients, local media and the secretary of the Dept. of Health and Human Services. If you have breach insurance, all the costs associated with the breach would be covered: the cost to notify the victims, to investigate the breach, to pay the government fines, to pay your legal costs and to cover any other damages. Some of these policies also pay for a public relations firm to restore your good name.
Talk to your professional liability insurance carrier to see what protection you currently have. Malpractice insurance covers many types of risk and may be broad enough to cover HIPAA security breaches.

Good luck!

Attachments
#1: “How to Write Your Office Privacy Policy”
#2: “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 your “Notice of Privacy Practices” and 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. Keep our computer systems safe by not clicking on a suspicious link on a website or in an email, opening a suspicious e-mail attachment or going to a suspicious website. You could accidentally allow a hacker to infect or steal our patients’ PHI.

10. Any violations of the Privacy Rule, our the state’s 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.

11. 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.

12. 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.

If you lose a device that includes PHI, the practice can be investigated for HIPAA violations and fined hundreds of thousands of dollars.

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.

Written by ___________________ Approved by ______________________

Attachments:
1. “Notice of Privacy Practices”
2. “ABC Clinic Security Procedures”

__________________________ __________________________
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 _____________________
THIS BUSINESS ASSOCIATE AGREEMENT, made and entered into this ____________ day of ____________, 20____ (“Effective Date”) by and between ___________________________ , hereinafter referred to as “Business Associate”; and ____________________________________________ hereinafter referred to as “Healthcare Practice.” Each party may be referred to individually as a “Party” and collectively as the “Parties.”

WHEREAS, Business Associate has been engaged to provide management consulting and coaching services to Healthcare Practice. Healthcare Practice wants the option to share, review and/or discuss Protected Health Information (“PHI”) with Business Associate for practice management purposes; and

WHEREAS, the Parties have a relationship that may qualify as a business associate relationship under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160, Subpart A, and 45 CFR 164, Subpart E (collectively, the “Privacy Rule”), the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 164 Subpart C (the “Security Rule”), and the Standards for Notification in the Case of Breach of Unsecured Protected Health Information at 45 CFR Part 164 Subpart D (the “Breach Notification Rule”); and

WHEREAS, the Parties desire to enter into this Agreement to comply with HIPAA, the Privacy Rule, the Security Rule, and the Breach Notification Rule and to set forth the various business associate responsibilities of Business Associate as more particularly set forth herein.

The parties agree as follows:

1. Security and Confidentiality. If Business Associate receives any PHI as defined in 45 CFR 160.103 from Healthcare Practice, or creates, receives, maintains or transmits any PHI on behalf of Healthcare Practice, Business Associate shall maintain the security and confidentiality of such PHI in accordance with all applicable laws and regulations, including, but not limited to, HIPAA, the Privacy Rule, the Security Rule, the Breach Notification Rule and any other regulations promulgated under HIPAA, and as otherwise “Required by Law” as such term is used in 45 CFR 164.103. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in 45 CFR 160.103, 164.103, 164.402, and 164.501.

2. Required Disclosure. If required by law, 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 Parties compliance with the law.

3. Limitation on Use and Disclosure of PHI. Healthcare Practice agrees to disclose PHI to Business Associate the minimum amount of PHI necessary for the Business Associate’s purposes. Business Associate shall not use or disclose PHI otherwise than (i) to provide Services, as expressly permitted by this Agreement, (ii) to satisfy its obligations under this Agreement, or (iii) as Required by Law. Except as otherwise limited by this Agreement and provided such use or disclosure would not violate the Privacy Rule if done by Healthcare Practice, Business Associate may use or disclose PHI to provide Services for or on behalf of Healthcare Practice. Business Associate hereby acknowledges and agrees that as between Business Associate and Healthcare Practice, all PHI shall be and remain the sole property of Healthcare Practice, including, but not limited to, any and all forms thereof developed by Business Associate in the course of fulfillment of its obligations hereunder. Business Associate represents that, to the extent Business Associate requests that Healthcare Practice disclose PHI to Business Associate, such a request is only for the minimum PHI necessary to accomplish Business Associate's purpose.
4. Safeguards. Business Associate shall implement, maintain and use all appropriate safeguards to prevent the use or disclosure of PHI other than as permitted by this Agreement, including administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic PHI as defined in 45 CFR 160.103 that Business Associate creates, receives, maintains, or transmits on behalf of Healthcare Practice. Business Associate shall develop policies and procedures and implement the requirements of the Privacy, Security, and Breach Notification Rules as applicable to Business Associate.

5. Reporting of Violations. Business Associate shall immediately, in any event, within fifteen (15) days of discovery, report to Healthcare Practice (i) any use or disclosure of PHI not provided for and permitted by this Agreement and the Privacy Rule; (ii) any security incident involving electronic Protected Health Information; and (iii) any Breach of Unsecured Protected Health Information of which it becomes aware. Such notification shall include the identity of the individual who is the subject of the Breach, together with any other information Healthcare Practice determines necessary. Business Associate shall mitigate, to the extent practicable, any harmful effect of any use or disclosure of PHI by Business Associate in violation of this Agreement.

Business Associate shall be responsible for all costs and expenses incurred by Healthcare Practice in notifying individuals, the media, and the Secretary of the Department of Health and Human Services of a Breach where the PHI was maintained, used, or disclosed by the Business Associate when the Breach occurred.

6. Termination of Agreement. Notwithstanding any other provision of this Agreement to the contrary, either Party may immediately terminate this Agreement and any oral agreements upon the provision of written notice to the other Party.

7. Return or Destruction of PHI when Agreement Ends. Within thirty (30) days of expiration or earlier termination of this Agreement, Business Associate shall return or destroy all PHI. Business Associate shall not retain copies of any PHI. This provision shall also apply to PHI in the possession of any subcontractors or agents of Business Associate. Business Associate shall provide a written notice that all such PHI has been returned or destroyed.

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

9. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Healthcare Practice to comply with the Privacy Rule, the Security Rule, and the Breach Notification Rule.

10. The rights and obligations of Business Associate of this Agreement shall survive the termination of this Agreement. A faxed or scanned copy of this Agreement shall be considered as valid as the original copy.

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement to be effective on the Effective Date.

Healthcare Practice

By: ______________________________________  By: ______________________________________
(Print Name and Title)

Date: ______________________________________   Date: ______________________________________