HIPAA & Privacy : A Survival Guide to the Law
Volume 2011, Course No. 301
Self-Study Course #110301

The Health Insurance Portability and Accountability Act (HIPAA) affects almost every aspect of the healthcare industry. There are many different components of HIPAA including security, transactions, privacy, training, etc. Various parts of HIPAA affect different areas within healthcare. A whole industry has been established to interpret, train, implement, and analyze HIPAA's impact.

HIPAA was born in 1996. "Electronic medical records" had just become a catchphrase. The government wanted to standardize the electronic transmission of billing and claims information, but at the same time they recognized that this increased the risk of abuse of patient's private information. This meant that comprehensive federal laws were needed to protect this health information for the digital age. The bottom line of HIPAA is that healthcare providers and health plans must protect patient information. Providers and plans may not use or disclose an individual's health information except for treatment, payment, or regular healthcare operations. Any additional use of a patient's healthcare information requires an authorization signed by the patient.

The original intent of HIPAA makes sense. The ultimate goal is to make it easier for consumers to receive seamless care no matter which provider they see. Providers and patients should all have access to important patient medical information. And, while making the information available, HIPAA protects patient privacy and confidentiality as much as possible...without hindering the access to, and quality of, healthcare.

These privacy protections give patients federal rights that guarantee they can inspect their medical records, correct mistakes, inquire who has seen their records, and seek penalties if their health information is used inappropriately. It also strictly controls the use of medical information for marketing.

But the privacy rules still allow personal medical information to be shared for basic healthcare operations, such as treating patients and transmitting claims for payment. HIPAA requires healthcare providers to make their best efforts to protect patient medical records and share the smallest amount of information needed. This isn't a major shift in the general practice of many healthcare professionals. Pharmacists and prescribers have always been aware of the importance of protecting medical records. Hospitals and physician offices use consent forms for the release of medical records.

> The American Pharmacists Association Code of Ethics says: *With a caring attitude and a compassionate spirit, a pharmacist focuses on serving the patient in a private and confidential manner*.
>
> The American Medical Association Code of Ethics says: *A physician shall respect the rights of patients, colleagues, and other health professionals, and shall safeguard patient confidences and privacy within the constraints of the law*.

All healthcare providers are required to be compliant with the privacy and security rules put forth in the Health Insurance Portability and Accountability Act (HIPAA). Plus the American Recovery and Reinvestment Act of 2009 (ARRA) contains significant changes to the original HIPAA rules. This activity is designed to give you a better understanding of the HIPAA Privacy Rule. The Security Rule is covered in *HIPAA & Security: A Survival Guide to the Law*.

Introduction

HIPAA training is required for each person with access to confidential patient information. This activity is intended to help you meet that requirement and help you gain an understanding of the basic concepts and terminology involved with HIPAA.

This activity is NOT designed to address the issues that will be faced by corporate management, hospital management, attorneys, or HIPAA Privacy Officials. It is also NOT intended to represent legal advice. For detailed information and advice necessary for these individuals and questions, we recommend more specific resources. A list of resources and manuals that delve deeper into the privacy rules is provided at the end of this activity.

Who Does HIPAA Cover?

Covered Entities

"Covered entities" must abide by HIPAA requirements. This means any person, business, or institution that provides healthcare or keeps records on patients (pharmacies, physician offices, other healthcare providers, health plans, billing services, etc). All practicing pharmacists and prescribers with direct relationships with patients are covered entities and must comply.

Hybrid Entity

This applies to an entity in which part of the entity is covered by HIPAA while other parts are not.

For example, a discount department store might have quite a few employees working in the "front end" and fewer employees working in the pharmacy or walk-in clinic. The "hybrid entities" concept means a department store could remain legal by providing the required training to employees of the clinic and/or pharmacy. They don't need to provide HIPAA training to clerks and others who work in the "front end" of the store, as long as the necessary "firewalls" are in place to keep patient health information in the pharmacy and clinic area.

Another example would apply to a hospital. A hospital would not have to apply the HIPAA training to employees who work in parts of the hospital that don't have anything to do with patient privacy. A person working in the gift shop doesn't have to be trained on HIPAA, but the hospital does need to protect patient medical information from being accessed by their non-clinical employees.

Most hospitals and pharmacies are hybrid entities and therefore allow for some employees to be trained, while others are not. A small pharmacy or prescriber's office that does nothing but provide healthcare may not be considered a hybrid entity, so all employees need appropriate HIPAA training.

Direct Treatment Relationship

Parts of the law apply to healthcare providers who have a direct treatment relationship with a patient. This includes a provider offering products or services to the patient. Other parts of the healthcare industry do not have such a relationship. For example, a university research laboratory technician might be working on a patient's blood sample, but does not have a direct treatment relationship with the patient, and therefore follows somewhat different rules.

Anyone practicing in a prescriber's office or pharmacy, and providing services to patients, has a "direct treatment relationship" and needs to follow the appropriate parts of the law.

Privacy Official

HIPAA requires that each covered entity must appoint a Privacy Official, who is responsible for developing and implementing company policies to comply with the privacy rules. There also must be a contact person or means in place for patients to submit complaints and ask questions about privacy issues. The contact person and the Privacy Official can be the same person. Chain pharmacies or affiliated hospitals that are under common ownership only need one Privacy Official and/or contact person for the whole group. Make sure you know who your Privacy Official is...and how to get in touch with him or her.

All companies must develop and maintain written or electronic policies and procedures detailing their HIPAA related rules. These policies and procedures must be maintained for 6 years from the date of their development or the last date they were in effect, whichever is later.

Protected Health Information (PHI)

You'll hear a lot of people adding "PHI" to their healthcare alphabet soup. Protected Health Information refers to any patient information in any form that:

1. is created or received by a covered entity;
2. relates to a patient's health condition in the past, present, or future; and
3. identifies the patient.

PHI is any information transmitted or maintained in any form, such as lab results, visit notes, prescription records, billing records, and oral communications on the phone or during patient counseling. In 2008, a clarification of the Privacy Rule spelled out that PHI includes genetic information too. The Genetic Information Nondiscrimination Act of 2008 or GINA protects people from being discriminated against by their insurance company on the basis of genetic testing they've had. A provision of that law lists genetic information as health information under HIPAA, but does not allow it to be used for determination of eligibility, premiums, or pre-existing conditions.

Keep HIPAA requirements in mind any time you are handling any health information that pertains to a patient.

Protected Health Information (PHI) includes information that is:

- Spoken
- Written
- Electronic

You can continue to report adverse drug events under the HIPAA Privacy Rule. The Rule is not intended to disrupt or discourage adverse event reporting in any way. In fact, the Privacy Rule specifically permits covered entities (such as pharmacists, physicians, or hospitals) to report adverse events and other information related to the quality, effectiveness, and safety of FDA-regulated products both to the manufacturers and directly to the FDA.

Pharmacies need to keep in mind that discarded labeled prescription vials contain PHI and need to be handled with care. Pharmacy chains have been the subject of multi-million dollar lawsuits after employees at some stores left labeled prescription vials in open trash containers outside the store. Either the labels should be removed from returned prescription vials and shredded or the vials should be kept in opaque bags in secure areas until picked up by a disposal vendor who is contracted to shred or otherwise destroy them.

De-identified Health Information

HIPAA does not apply to de-identified health information. De-identified health information refers to patient information that CANNOT be used to identify an individual. Privacy rules DO allow giving out such health information without patient authorization in certain situations and when identifiers are removed, such as names, street addresses, social security numbers, email addresses, telephone and fax numbers, license numbers, full face photographs, medical ID numbers, fingerprints, etc. De-identified information can include city, state, zip code, date of birth, and date of death. These "limited data sets" can be used for research, public health purposes, quality improvement activities, or healthcare operations within the pharmacy or clinic practice. If your pharmacy or practice plans to release limited data sets for research, make sure that the information is "de-identified" and that the researchers have signed a Data Use Agreement that meets HIPAA requirements.

De-identified information under HIPAA:

1. City, state, zip code of patient's address
2. Patient's date of birth
3. Patient's date of death

Minimum Necessary

One standard prevalent in HIPAA is that patient privacy should be protected by minimizing the amount of private information that is given out about a patient, and minimizing where the information is sent. This concept is often referred to as "minimum necessary." The privacy rule requires a reasonable effort to limit PHI to the minimum required to accomplish what needs to be done. Keep this concept in mind and apply it whenever dealing with PHI. For example, if you are submitting a claim for a patient, do not automatically provide the diagnosis unless the payor needs that information.

The rules say that whatever information the payor asks for will be considered to be the minimum

necessary unless the provider disagrees. If, in your judgment, the information that the payor asks for is not the minimum necessary, you are supposed to negotiate with the payor to agree upon the minimum necessary information. This depends on your judgment and you do not have to provide information that you do not think meets the requirement of being the minimum necessary.

Keep in mind that the payor does not have to pay you though. This means that you might win the battle...meaning you do not divulge information you don't feel is necessary...but the payor might win the war...because they don't have to pay you if they don't get the information they want from you.

Only request what PHI you need to know...and only disclose what is required. But HIPAA does allow for certain exceptions to the minimum necessary rule. For example, the minimum necessary requirement does not apply when talking directly with the patient or any disclosures that fall under a written authorization from the patient. Other exceptions are discussed in the text box.

Minimum necessary exceptions:

1. Use by a healthcare provider for treatment purposes
2. Use by the individual patient or uses authorized by the patient
3. Uses or disclosures required for HIPAA compliance
4. Disclosures to the Department of Health and Human Services (HHS) under the Privacy Rule
5. Uses required by other laws

"Minimum necessary" is also designed to encourage your pharmacy or practice to evaluate who should be accessing patient records. If support staff doesn't need patient medical records to do their jobs, don't give them access to the records.

Company policies and procedures should identify:

The types of people who need access to PHI to carry out their jobs
The types of confidential information that these individuals need to perform their duties, and
Under what conditions these individuals need access to PHI

It’s important to note that pulling up your own medical information is not appropriate. It’s not appropriate to pull information on a friend or family member either, even if they’ve asked you to do so. You may have access to your medical records because you’re working (or doing a rotation) in the same location or health system where your records are stored. If you want to review your records, you must go through the same process as any other patient.

The goal is to limit access to PHI to those who need it and to exactly what parts they need to do their job. Companies often develop standard protocols that govern the confidential information disclosed or requested and keeping it to the minimum necessary to achieve the desired purpose. The advantage of written policies and procedures is that once the policy is set each request doesn't have to be reviewed individually. However, requests not covered by policy will still need to be reviewed on a case-by-case basis.

Examples of POOR privacy judgment:

Photos of a dying patient posted to Facebook - resulted in 4 hospital staff members being fired and 3 more being disciplined. The internet is not the place to post pictures of patients.
Patient records found intact at a local dump (including social security numbers, names, addresses, diagnoses, etc) - resulted in a hospital internal review and a telephone hotline for patients. Appropriate disposal of PHI is mandatory.
Discussions about patients posted to Facebook - resulted in termination and termination hearings for involved employees. Even without PHI disclosure, some hospitals are taking a zero tolerance stance regarding discussion of patient cases on social media sites. Social media sites are NOT the place to discuss patients, even if you aren't releasing PHI.
30,000 printouts of hospital records containing PHI were sold for $40 to a paper recycling center - resulted in a janitor being charged with felony commercial burglary. Although the involved party maintains he was just trying to sell paper for the recycling money, clearly THAT paper wasn't supposed to leave the hospital.

Disclosure

HIPAA rules stipulate to whom you can and cannot give information. One concept is that you CAN disclose information to another healthcare provider as long as the other healthcare provider has a treatment relationship with the patient and has informed the patient of their own privacy policy. This means you can always call another provider who is caring for a patient to discuss the patient and freely trade PHI back and forth. The concept of "minimum necessary" information does NOT apply to these sorts of communications. The law does not want to inhibit your communication with another provider in a way that would make it harder for you to act in the best interest of your patient.

HIPAA does permit some incidental disclosure of information, such as announcing a patient's name in a waiting room or having a patient's chart on an exam room door. It even allows friends or family members to pick up prescriptions for a patient. But the pharmacist is required to use professional judgment and look out for the patient's best interest when allowing someone else to pick up the prescription. Keep the necessary information to a minimum and invite the patient to call you by phone if they have any questions or need counseling.

HIPAA also allows health professionals, at their discretion and with certain limitations, to speak to relatives, friends, or caregivers...unless the patient specifically requests them not to. Keep the patient's best interest in mind when discussing their health information with relatives, etc., and only discuss items pertinent to the current health condition.

Don't be afraid to announce a patient name in a waiting room or pharmacy. Just keep it to the minimum: "Mrs. Lamberjack, please return to the pharmacy." Don't announce any health-specific information, such as a condition or drug name.

Disclosure of patient health information is allowed under certain circumstances, such as for public health activities; victims of abuse, neglect, or domestic violence; law enforcement purposes; to comply with workers' compensation; to avoid serious threat to health or safety; for specialized government; to DEA investigators, or state pharmacy board inspectors; and to report adverse events or other drug- or device-related problems to FDA. Keep in mind that in civil matters, such as divorce

proceedings, patient-related health information should only be turned over pursuant to a subpoena or appropriate legal document. All requests for the release of PHI in these circumstances should be forwarded to the Privacy Office/Official for their review.

Many health professionals have heard about HIPAA regulations and are very concerned that they will be in violation if some information is overheard by another person when they are counseling a patient or a piece of paper is seen by somebody who should not see it. HIPAA does allow for incidental disclosures as long as policies are in place to protect patient information. For example, you wouldn't be in violation of the law if you were talking with a patient in a semi-private counseling area or discussing the patient's condition at a nurses' station, and someone accidentally overhears you. Keep in mind that this type of accidental disclosure is only okay if it couldn't be reasonably prevented...is limited in nature...and is an unintended result of a permitted disclosure. HIPAA permits these accidental disclosures of PHI if there are reasonable safeguards (administrative, technical, and physical) in place to protect patient privacy.

The HIPAA Privacy Rule MAY NOT be violated if a disclosure:

1. Couldn't reasonably be prevented,
2. Is limited in nature, and
3. Is a byproduct of permitted disclosures

HIPAA does allow the transfer of patient medical records in the event of a change of ownership. So if you work in a pharmacy that is being bought, the patient information automatically goes to the new owner. Under this circumstance, patient authorizations to transfer their records are not required by HIPAA.

It is important to use good judgment, and try to protect patient health information, but HIPAA takes into account that it is unreasonable to control every possible situation in which the information could leak out.

Each company must inventory and categorize its disclosures and uses of PHI in its policies and procedures into three categories:

Internal use
Routine disclosures
Non-routine disclosures

Permitted PHI disclosures:

1. To the individual patient
2. For treatment, payment, healthcare operations
3. With opportunity for the patient to agree or object
4. Incidental to an otherwise permitted use and disclosure
5. Public interest and benefit activities, which include court orders, victims of abuse, neglect, or domestic violence, law enforcement activities as well as public health
6. Limited data set for research, public health, or healthcare operations

When documenting non-routine disclosures make sure you include:

- The date
- The name of the person or entity you disclosed the information to
- Their address, if you know it
- A description of what was disclosed
- A statement of the reason PHI was disclosed that is designed to reasonably inform the patient why you disclosed their information

Complaint Process

HIPAA requires that each company have a specific process to deal with complaints from anyone who believes their privacy has been violated. But understand that complaints about privacy violations or privacy policies of your company aren't required to be voiced to an employee. They may be submitted directly to the Secretary of the Department of Health and Human Services.

If you receive a complaint, you should be prepared to direct the person to the individual or department at your company charged with documenting complaints. All complaints must be documented, including their outcomes and all documentation maintained for at least 6 years.

Complaints can come from anyone - a patient, an employee, an anonymous tip, etc. Each must be handled appropriately and not ignored. Be familiar with your company's policy concerning HIPAA-related complaints.

Complaints may result in a change in company policy, and for those violating patient privacy serious disciplinary actions may result, up to and including termination.

Accounting of Disclosures

Patients can ask you to give them a list of any instance, going back six years or less, in which their information was disclosed to anybody outside the realm of treatment, payment, or regular operations. This means that you have to keep records of who you sent information to for at least six years. Once requested by a patient, you have 60 days to provide them an accounting of these disclosures, including the date, name, and address of who you gave the information to, brief description of the disclosure, and the reason for it. You can get a 30 day extension if you provide the patient with a written explanation of the delay and the date they will receive the accounting. Remember this is only for non-routine uses. Non-routine disclosures are defined by the Privacy Official and include any disclosure not considered by the entity to be a routine disclosure.

You do not have to account for disclosures that have to do with treatment, billing, accounting, or conversations you had directly with the patient. Unintended disclosures of patient health information also do NOT need to be documented and included in the list of disclosures. For example, if someone accidentally overhears a conversation you are having with a patient, you don't need to document it as a release of PHI. And you don't have to track or account for those you are legally required to make, such as to a court under a subpoena or other law or governmental authorities. Accounting is also not

required if the disclosure is made pursuant to a patient authorization.

Be sure to keep a record of times you give out information on any patient, for a non-routine use, and be prepared to give this information to a patient if it is requested. Patients also have the right to a copy of any written requests you receive to release their confidential information, so be sure to keep those requests on file too.

An accounting within any 12 month period must be provided free of charge, but you may charge for additional requests as long as you notify the patient in advance what the charge will be and agree to any modification the patient makes to the request after they find out the cost.

In addition to retaining the information required by the HIPAA accounting rules, you must retain a copy of the written accounting provided to the patient and the title of the person who received and processed the patient's accounting request for a period of 6 years.

Copies of Records

Patients also have the right to obtain a copy of their records. If you receive a request, you have 30 days to provide the patient with a copy. Patients can also request a change to their records. It's best to ask the patient to put the request in writing and include the reason for the change. You must act within 60 days to determine whether the change is appropriate and then correct the records if necessary. For example, say a patient denies receiving a prescription for haloperidol. Under the privacy rules, you might be required to check your records to see if this is a real error before updating the patient's medical record. Before you delete any health information from a patient's record, make sure the removal of the information is consistent with other laws or your organization's general practices.

Consent

After HIPAA was enacted there was a lot of talk about being required to get the patient's signed consent before doing anything with any patient information. This requirement was eliminated. You do not need to get the patient's consent before you process their information. One reason this concept was eliminated was to accommodate prescriptions faxed or called into a pharmacy. The worry was that information on new prescriptions could not be used in a pharmacy if there was no signed consent form on file. Basically, a pharmacist couldn't talk to a prescriber's office to take a prescription.

The final privacy rules did away with mandatory consent. Consent is now only an OPTION. If your pharmacy or practice already uses consent forms for various purposes, it is okay to continue using them. The privacy rules don't have specific requirements for what should be included in a consent form, so no changes forms are necessary based on HIPAA.

Notice of Privacy Practices

HIPAA relies on giving a "Notice of Privacy Practices" in place of obtaining the patient's signed "consent." You do not have to have patients give their signature and authorize you to use their private information. You just have to give them the written Notice of Privacy Practices. If your pharmacy or practice continues using consent forms, they are still required to also provide a Notice of Privacy Practices.

The privacy notice is intended to create an initial moment and spur discussion between you and your patients concerning how you will use their PHI. This provides an opportunity for patients to make requests for additional restrictions on the use of their medical information. A patient could request that no one other than themselves can pick up their prescriptions...or hospital staff cannot discuss their condition with family or friends. Document any additional requests on the privacy notice and make a note in the computer or the patients chart to remind you of their requests. As of February 17, 2010, if a patient requests you not release their PHI to a health plan, you must do so...as long as they've paid cash instead of using their insurance card. Previously a covered entity was not required to honor this type of request.

Keep in mind your patients' healthcare literacy. The Notice of Privacy Practices should be written in clear, simple language at approximately a sixth grade reading level. Patients may not readily volunteer that they don't understand the privacy information. Briefly explain the notice as you give the form to a patient and offer an opportunity for questions. If your practice serves multicultural patients, having different language versions of the notice is also helpful.

The federal government wants the privacy notice to be specific for your pharmacy or practice. They don't want to see everybody using the same model policy. In other words, you must have a policy stating how YOU protect patient information, and who YOU will or will not give the information to. A single privacy notice can cover all the pharmacies in a single chain or all the departments of a hospital.

With the addition of genetic testing results to the list of PHI, health plan privacy notices now need to include that they won't use genetic information for underwriting purposes.

Requirements of a valid privacy notice are that it:

1. Be written in plain language (for example, a sixth grade reading level);
2. Describe, with examples, the types of disclosures to be made with or without patient consent or authorization;
3. When the covered entity is a health plan who normally uses PHI for underwriting purposes, it must include language explicitly stating that is the health plan won't use or disclose genetic information for underwriting purposes;
4. State that other disclosures require a patient's written authorization, which may be revoked at any time;
5. State that your pharmacy or practice is required by law to maintain the privacy of protected health information;
6. Explains to patients their rights, including their right to inspect and amend their records, to ask for accounting of disclosures containing their protected health information, to limit how their PHI is used, and how and when they want to be communicated with;
7. Alerts patients that they can complain to the Secretary of Health and Human Services;
8. Identifies the contact person regarding privacy issues; and

9. Contains the wording: "This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully."

You must give or mail this notice to your patients on the same day you first provide treatment or service. Patients must also indicate that they have received the information. This is quite different from having your patients indicate that they actually consent to your sharing their PHI with others.

Hand the privacy notice to the patient at your first face-to-face meeting. If you are providing products or services without face-to-face contact, such as offering advice or counseling them on the phone, you must mail the notice to the patient on the same day. In emergency situations, the notice needs to be delivered as soon as reasonably practicable after the emergency. If you have a website that patients can go to, you need to make sure the privacy notice is available as a link. You are also required to post a copy of your privacy notice in an easy-to-view area of your pharmacy or practice, such as a waiting area or check-in desk.

You must make a good faith effort to obtain acknowledgment from the patient that they have received your privacy notice. The patient can initial the notice, sign a list, or complete a separate document. If you have a website, you can have the patient click a box on an electronic form, use a digital signature, or anything that requires some affirmative action on the part of the patient. You can use a "layered" notice, which consists of two versions...a short summary of the patient's rights...and the full notice explaining all the required information. Patients can initial or sign the summary and hand it to you for acknowledgment...and keep the full notice for their records. You can also send the notice home with the relative or friend who is picking up the patient's prescription. Have the patient either mail in their acknowledgment or drop it off at their next visit.

When patients sign or initial a log book acknowledging that they have received a copy of your policies, make sure the individual is clearly informed of what they are acknowledging...but there is a very specific kicker that you must be aware of. You CANNOT combine this acknowledgment with a waiver for something else. For example, in a pharmacy, you CANNOT have a patient initial or sign that they have received your privacy policy AND waive the requirement for counseling under OBRA with one initial or signature. You have to get them to initial or sign for each separately. This may require one log book that accepts two separate signatures...or two separate log books.

Keep in mind one very important point. Patients are NOT required to sign or acknowledge the privacy notice if they choose not to. But don't deny treatment or services if a patient won't sign the privacy notice. Just document your efforts and the reason why the patient did not sign the acknowledgment.

Once a patient has received your privacy notice, they will not have to acknowledge it again. Anytime a significant change is made in the privacy notice, it must be reissued. This means that the new Privacy Practice Notice should be posted, which includes updating postings on your company's website, and provided the new version to patients upon request. But you are NOT required to physically redistribute the notice every time it's revised.

Keep all of the patient acknowledgments of your privacy notice on file for at least 6 years.

Minor's Rights

If you have a minor who is receiving birth control pills, treatment for a sexually transmitted disease, or mental health treatments, etc., can you divulge information about this to the parents, if the parents

ask? Sometimes yes...and sometimes no.

HIPAA says you need to abide by whatever your state law requires. Therefore, you need to know if your state law, or other applicable law, allows you to divulge this information or not. Most state laws do not stipulate. HIPAA says that if your state does not specifically allow or disallow release of this information to parents of a minor, then it is up to the provider's professional judgment.

Newborn screening for hearing and metabolic issues is conducted before babies leave the hospital. This information may be shared under the umbrella of public health.

Information for Marketing

Most of the concepts discussed so far apply to using a patient's private health information in a manner related to the care of the patient. A whole set of new rules comes into play if the information is going to be used for marketing purposes.

If you are going to release any patient information to be used for marketing purposes, you MUST have authorization from the patient. This is completely different than just having your patients acknowledge that they have received a copy of your privacy policy. You cannot put in your privacy policy that you will release information for marketing purposes and expect this to cover you. The patient must sign a release authorizing the use of their information for marketing purposes in addition to the patient's acknowledgment of receiving a copy of your privacy policy.

There are specific definitions of what constitutes marketing. The law says that marketing means to make a communication about a product or service that encourages the person to purchase or use the product or service.

But, the most important part of this rule is the EXCEPTIONS.

You CAN provide all sorts of information to the patient that is NOT considered marketing. For example, you can inform patients about formulary restrictions or other features and benefits of their health plan. You can give them information about other treatments that are specific for them. You can give them any sort of general health communication, for example, how to care for diabetes, how to lower their blood pressure, etc.

Any communication that relates to the treatment of the individual is not considered marketing. For example, you can send patients appointment or refill reminders. This could seem confusing because the reminders might seem like they are designed to promote purchase or use of the product or service, but the fact that they pertain to the treatment of an individual patient makes these reminders exempt and perfectly okay. You also CAN recommend things such as generics, or different healthcare providers, or different alternatives, because they are considered part of your treatment for the patient, and therefore, are not considered marketing.

Be careful not to violate the anti-kickback statute. If you recommend a product or service, and you stand to make financial gain from it, and that service is paid for in part or in whole by the federal government, you would be committing a criminal act. For example, don't ever recommend a particular drug that you are getting paid by the drug manufacturer to recommend. Some of the patients you recommend it to might be getting coverage or reimbursement through a federal government program. You then could be guilty of violating the anti-kickback law and be subject to jail time for a criminal act. If you are using information for marketing purposes, and you are receiving any remuneration as a result of the marketing activities, you must mention this in the patient authorization form to release their information.

Authorizations

Before you use or disclose protected health information that is not considered an exception under HIPAA (treatment, payment, or healthcare operations), such as for marketing, you need to get a valid authorization from the patient. It is very important to remember you can no longer use "opt out" programs...that is to automatically enroll a patient in a program and give them the ability to "opt out" if they desire. You must have the authorization signed and in hand before performing "marketing."

In general, an authorization form must contain specific elements, such as:

- Description of the information to be used or disclosed
- Names of the individuals or entities who are giving and receiving the information
- Purpose of the disclosure
- An expiration date for the use of the information

For managers, owners, or Privacy Officials who need to create a model authorization form, refer to the more detailed resources listed at the end of this activity.

When filling out an authorization form to disclose patient info, keep a couple of things in mind.

- If the patient is requesting you release their records to someone, the patient is NOT required to state the exact purpose for the release. You can just write in that the patient is requesting it.
- If you are completing an authorization form for marketing purposes, ALWAYS include any remuneration you will be receiving for releasing protected health information.
- If a patient refuses to sign an authorization, you CANNOT refuse to treat them.
- An authorization needs to be a separate individually signed and dated document.

Emergency Situations

HIPAA allows sharing of PHI under emergency situations such as natural disasters where people may be evacuated and require healthcare. PHI may be shared with other providers for treatment or referrals. Information may also be given to emergency workers to assist in coordination of care. This also includes information required to coordinate payment for care.

In a disaster situation, providers may also share information that allows people to know the whereabouts and condition of their loved ones. Getting verbal permission is recommended, but if that is not possible, the provider must use their best judgment. This includes notifying the police, media, and disaster relief organizations like the Red Cross of identifying information regarding specific patients.

The U.S. Department of Health and Human Services Office of Civil Rights offers an online decision tool to help you determine if it's okay to release PHI in emergency situations.

Transaction Standards

HIPAA requires that certain electronic transmissions be standardized. The Privacy Official, information technology specialists, and upper management will make sure transaction standards are in place. If you are the Privacy Official or owner of a small pharmacy or practice, contact your

computer vendor to see if your system can support electronic transactions. E-prescribing and electronic medical records must maintain HIPAA privacy standards.

E-prescribing is a major part of nationwide Medicare initiatives to improve care and provide new services through health information technology. These initiatives were announced in July 2004 by the Centers for Medicare and Medicaid Services (CMS). The Medicare Modernization Act (MMA) of 2003 mandates that drug plans participating in the Medicare Part D prescription drug program must support the standards of e-prescribing set by the CMS by 2009. Adherence to an initial set of well-established standards was required by January 2006. The initial standards require drug plans that participate in the Medicare prescription benefit to support electronic transmission of prescriptions, information on eligibility and benefits (e.g., drug formulary, prior authorization messages), and patient instructions.

Participation of prescribers and pharmacists is voluntary. As a result, e-prescribing has been slow to catch on due to the expense of software/hardware to support e-prescribing and the time needed to learn how to operate the system. It is estimated that about 25% of prescribers are using e-prescribing currently, but this number is expected to increase now that the DEA is allowing e-prescribing of controlled substances. At the end of 2009 about 85% of pharmacies were connected electronically for e-prescribing.

In addition to e-prescribing, electronic medical record (EMR) systems help improve record keeping, recording, and documentation of office examinations, communication between clinicians, and office workflow. The improved documentation and record keeping can potentially lead to higher reimbursement. A recent study of the potential impact of outpatient EMRs estimated there is a 40% reduction in erroneous claims, primarily by flagging missing diagnostic codes and inferring appropriate correction from analysis of the patient's record.

There are many e-prescribing choices for prescribers. The spectrum of choice depends on the extent of electronic prescribing integration. A stand-alone prescribing system will enable new prescription prescribing, including checking for patient eligibility and third-party formulary coverage, transmission of the prescription to the patient's pharmacy, and an automated refill authorization process. A comprehensive electronic medical record (EMR) system has e-prescribing features and also automates the entire medical record system.

The terms electronic medical record (EMR) and electronic health record (EHR) are often used interchangeably. However, these two terms describe different concepts. The EMR consists of a clinical data repository, clinical decision support, computerized provider order entry, pharmacy, and clinical documentation applications. EMR is used by healthcare professionals to document, monitor, and manage healthcare delivery within a care delivery organization (e.g., hospitals, clinics). The data in the EMR document tell what happened to the patient during their encounter at the care delivery organization and is owned by the care delivery organization. It does not contain other care delivery organization information.

Electronic health record (EHR) is a subset of each care delivery organization's EMR. It is owned by the patient and has patient input and access that spans different care encounters across multiple care delivery organizations within a community, region, or state. It provides interactive patient access. The

EHR can be established only if the electronic medical records of various care delivery organizations have evolved to a level that can create and support exchange of information between one another within a community or region.

The concerns of security and confidentiality with e-prescribing were valid since some vendors had initially stated that patient information and physician prescribing data would be shared with third parties for commercial purposes. However, now vendors are legally required to not divulge any patient information to third parties as mandated by HIPAA. And e-prescribing is relatively secure as e-prescribing systems and electronic health records typically employ multiple layers of privacy protection. The tools and techniques used to secure information are the same as those used to protect credit card transactions.

According to the Department of Health and Human Services (HHS) final ruling on e-prescribing, the security of e-prescriptions, and the protection of e-prescription information must meet the requirements set forth under HIPAA's administrative provisions for PHI and electronic protected health information (ePHI).

HIPAA Training Requirements

All employees with access to PHI must receive HIPAA training soon after hiring and companies are responsible for maintaining documentation of training completion for a period of 6 years. Training can include programs such as this one PLUS training on company specific policies and procedures relating to the HIPAA Privacy Rule.

If significant changes are made to the HIPAA Rule or company's policy and procedures, all employees affected by the changes must receive updated training in a reasonable amount of time after the change becomes effective

Business Associates

Companies have to sign contracts with business associates to ensure that PHI is protected when a business associate employee is using it. Business associates include any person you release PHI to in order to perform a task for you. These tasks may include claims processing, data analysis, administration, utilization review, practice management, billing, quality assurance, etc.

The definition of business associate has also been expanded to include companies that provide data transmission of PHI to covered entities, when these companies need to routinely access that PHI. This would include health information exchange organizations, regional health information organizations, and vendors of personal health records.

Business associates of covered entities now have increased responsibility and liability. Previously they only had to be compliant with the parts of the Privacy Rule that were in their contracts. They now have to do all the same things that covered entities do to stay compliant with HIPAA...create a privacy policy, appoint a Privacy Official, etc. Plus they will be liable for any unauthorized disclosures and face the same penalties that covered entities do.

Contracts are not required between your company and its employees, volunteers, trainees, or others that perform duties under the direct control of your company, even if they aren't paid for their services. They are also not required between treatment operations, such as between physicians in a hospital, or between a group health plan and plan sponsors

Medical Identity Theft

Although not part of HIPAA, medical identify theft is an important concern that relates to PHI and is affected by HIPAA. Medical identity theft involves the use of an individual's personal information, without that person's knowledge or consent, to collect money, prescription drugs, medical goods, or health services. It's not only potentially damaging financially, but it can also be dangerous to a person's health. Medical identity theft can result in fictitious information and wrong histories and diagnoses being included in patients' charts and records. The incidence of medical identity theft is thought to be on the rise. It's speculated that up to half a million people have been victims. Although anyone, from neonates to the elderly, could be victimized, those who frequently access the healthcare system are most vulnerable. The patient handout included with this document will help make patients aware of medical identity theft, and give them the resources to prevent and rectify medical identity theft.

How Does It Happen?

Medical identity theft can result from something as simple as one person using another person's social security number (or social insurance number in Canada) and name for a hospital admission, procedure, or treatment. It can also happen when corrupt healthcare workers and organized crime rings file false claims with insurance companies for procedures and treatments that never took place.

Current evidence suggests that people with legitimate access to computer systems and/or patient data may often be the primary culprits in medical identity theft. While much of the responsibility of preventing medical identity theft lies in the realm of health information systems, there are common sense steps that healthcare professionals can take to reduce opportunities.

What Should Pharmacies Do?

Lawsuits have been brought against pharmacies that have improperly disposed of confidential patient information in unsecured dumpsters. This information included names and social security numbers of thousands of patients in several U.S. cities, and was certainly an opportunity for medical identity theft to occur.

HIPAA rules have forced some of the safety measures that healthcare companies take to prevent the release of private patient information. Some of these include special disposal of patients' old vials, locking of outdoor dumpsters, inspection of all trash to be sure that it doesn't contain private patient information, requiring all trash from the pharmacy be returned to company warehouse facilities for disposal, or shredding all trash that has private patient information. Regardless of the mechanism through which it is achieved, the goal is to be certain that personal information of patients is not disclosed to anyone other than the appropriate pharmacy staff.

Other precautions that are in place to protect patient information for HIPAA are also prudent. These include pointing computer screens away from public areas, and keeping discussions with or about patients as private as possible.

What About Prescribers?

Prescribers should keep in mind the same goal as pharmacists, to protect private patient information from being accessed by anyone other than appropriate healthcare professionals. Discard documents with private patient information in shredders or bins designated for confidential documents. If none are available, initiate their implementation.

There are reports of laptops with patient information being stolen from the homes and cars of physicians. Don't create this opportunity for thieves. See our companion CE, *HIPAA & Security: A Survival Guide to the Law*, for HIPAA requirements related to the security of electronic PHI. Keep patient charts closed when not in use, and remember to avoid leaving charts and patient information in unsecured or easily accessed areas. The black market value of a single medical record may be $60 to $70.

Physicians can experience theft of their professional identities for the purpose of committing medical identity theft. Takeovers of clinics by crime rings and cases of imposters posing as physicians for the purpose of fraudulent billing have been documented. There are reports of scams involving phone calls to physicians asking for sensitive identity information, like driver's license number, social security number, universal professional identification number, educational background, and birth date. The callers have represented themselves as Medicare audit or claims employees, Medicare fraud investigators, or employees of major insurance companies. Be aware of this and guard your personal and professional information.

What Can Patients Do?

Medical identity theft isn't easy to detect, so being vigilant and proactive is key. Once medical identity theft occurs, it can be challenging for victims to get copies of their medical records and to have the inaccurate information removed from their medical records. Unfortunately, HIPAA can inadvertently act as a barrier to achieving these things. For example, victims don't have the legal right to demand correction of medical information that was not created by their current provider or insurer. In addition, a person's medical information may be disseminated to multiple entities, making it difficult to correct all erroneous information.

Patients should always review the "Explanation of Benefits" (EOB) sent to them by insurers. If anything is wrong, like charges for services, office visits, or medical equipment that wasn't received, the insurer and provider should be contacted.

A list of benefits paid in a person's name should be proactively requested from insurers each year and reviewed for discrepancies, like services and goods that were not received. If any are found, the insurer and provider should be contacted.

An "Accounting of Disclosures" should be requested yearly. This is a record of the disclosures of a person's health information made by healthcare providers or insurers. This information may be helpful in tracking where erroneous information, if it exists, may have been circulated.

Keeping an eye on credit reports is important too. Victims of medical identity theft may have collection notices for hospitals, medical labs, or other medical services on their reports.

Individuals can request copies of their medical records, and keep their own personal copy. This can help a person detect discrepancies, and ensure that accurate information is available if medical identity theft occurs. Patients may hear about websites that allow them to keep their own electronic personal health records (e.g., HealthVault, HealthFrame, YourMedChart, PersonalMD, etc). While these sites may offer a convenient way for patients to keep track of their health information, they are not always subject to HIPAA's protections.

For victims of identity theft, the main goals should be to correct both credit reports and medical records.

Educating patients on ways to prevent and detect medical identity theft is important as well. Use our patient handout "Medical Identity Theft: What You Should Know" to provide patients with the information they need about this crime.

HIPAA Enforcement

Mandated Audits

HHS is now REQUIRED to conduct periodic audits of covered entities and business associates. Previously, they could conduct audits, but they didn't have to.

Penalties

HIPAA authorizes the Secretary of Health and Human Services to impose civil as well as criminal penalties to covered entities if they have violated HIPAA Rules. The penalties for violating HIPAA rules have become stiffer over time and State Attorneys General can impose additional fines too.

Civil Fines

Civil fines are assessed based on the circumstances surrounding the violation as categorized in the following tiers.

Tiers of civil financial penalties for covered entities and business associates:

> For violations where the person **did not know** and by exercising reasonable diligence would not have known they violated a HIPAA rule, the penalty for each violation is between $100 and $50,000, with the total amount imposed for similar violations equaling not more than $25,000 to $1,500,000 each calendar year, respectively.
> For violations due to **reasonable cause** and not willful neglect, the penalty for each violation is between $1,000 and $50,000, with the total amount imposed for similar violations equaling not more than $100,000 to $1,500,000 each calendar year, respectively.

For violations due to **willful neglect** that is **corrected**, the penalty for each violation is between $10,000 and $50,000 (not more than $250,000 and $1,500,000 each calendar year for similar violations, respectively).
For violations due to **willful neglect** that is **not corrected**, the penalty is at least $50,000 (but not more than $1,500,000 per calendar year for similar violations).

The final amount of the fine is determined by an assessment of the nature and extent of the violation and the nature and extent of the harms inflicted by the violation.

A covered entity can prevent the assessment of these civil penalties if it fixes the violation within 30 days of discovering it. This makes it important for you to be on the look-out for violations and report them quickly, so they can be fixed quickly.

Criminal Penalties

These can include fines up to $50,000 or imprisonment for up to 1 year, or both. If the crime is committed under false pretenses, the fine can be up to $100,000 or imprisonment for up to 5 years, or both. If the offense involves a person obtaining or disclosing PHI with the intent to sell, transfer or use the information for commercial advantage, personal gain, or malicious harm the fines can be up to $250,000 or imprisonment for up to 10 years, or both.

Criminal penalties depend on whether a person **knowingly** and in violation of HIPAA, **uses or causes to be used a unique health identifier** or **obtains or discloses identifiable health information** relating to an individual.

This highlights the importance that is being placed on protecting medical information from inappropriate use.

Patient Cut

In the future, you can expect to see patients harmed by privacy violations get a cut of the fines collected. HHS is working to create a way to do this by February 17, 2012.

State Laws

In some cases state laws may pre-empt HIPAA requirements. HIPAA sets the bar, not the ceiling. If state privacy law is stricter than HIPAA, you should follow state law. HIPAA defines what it takes to be considered stricter:

Provides more restriction on a use or disclosure
Provides patients greater access or ability to amend their PHI
Provides patients more information about uses, disclosures, rights, and remedies
Narrows the scope, duration, privacy protections, or coercive effect related to authorizations
Requires longer or more detailed retention of records or accounting of disclosures
Provides patients greater privacy protection in any other way

However, when state law makes it impossible for you to comply with both sets of requirements (state and federal), or when state law is a barrier to you complying with the purposes and objectives of HIPAA, follow HIPAA not state law. But remember that you still need to follow the parts of the state law that don't conflict with HIPAA

Conclusion

As time goes on HIPAA continues to evolve and there are new rule for you to incorporate into your HIPAA toolkit. However, the basics don't change...use your common sense. HIPAA is really just legislated common sense to protect the personal, private and confidential information of patients. Try to protect the privacy of your patients' information as best you can. Think about where you are sending patient information...unintentional disclosures...how to handle patient complaints on privacy...disposal of certain information such as old prescription labels and vials...how best to leave information on answering machines...how to dispose of the trash...and similar situations. Even though the law does not address certain specific situations, and does not impose tight restrictions on you, it is appropriate for you to use your best judgment and minimize the potential for disclosing private health information. Also keep in mind that HIPAA doesn't override more stringent state privacy laws.

One easy tip to help you use patient information appropriately is to apply the "Mom Rule." How would you want your mother's PHI handled? Use your patients' PHI much like you would the private information of about a loved one. Help patients get the best care possible while protecting their health information from inappropriate use or disclosure.

Take a look at our *Colleagues Interact* discussions to chime in on HIPAA topics such as HIPAA Concerns...what you can tell patients over the phone or when someone other than the patient is picking up a prescription. Or, if you have questions or information to share, feel free to start a discussion of your own.

Here are HIPAA resources for further information:

Office for Civil Rights (DHHS)	The official government site for HIPAA news and updated guidances on the law
Agency for Healthcare Research and Quality	Government body involved with safety and privacy standards in healthcare information technology
National Committee on Vital and Health Statistics	Provides HIPAA updates and links to resources
American Medical Association	AMA HIPAA resource page, including sample forms and notices
American Society of Consultant Pharmacists	Resource page for HIPAA, including in-depth analysis of the rule
American Hospital Association	AHA HIPAA resource page, including sample forms and notices

The reader is responsible for utilizing professional judgment and confirming and interpreting the findings presented here before utilizing the information