

HIPAA – What’s legal and what’s not

Good afternoon everyone. My name is Lee Stickney. I am the Chief Executive Officer of the Health Care Resources Network (HCRNet). Thank you for coming today to learn about the law called HIPAA. And please always remember, it is a law and it carries penalties for violating it. The text for this lecture can be found on my web site, www.hcrnet.com, by clicking on member services, then click on HIPAA – what’s legal and what’s not.

Before we start, I want to talk about an old man in Seattle, Washington, sitting in a wheelchair dying of cancer. To make matters worse, he started receiving bills from credit card companies for cards he did not have. Besides having his identity stolen, he was concerned about his family having to pay these bills from his estate.

He went to the police and they told him it was basically useless to pursue the case because of the huge number of identity thefts.

He wasn’t willing to let go. He took the bills and went to the stores where the goods were purchased. He convinced some store managers to give him surveillance tapes showing the thief making the purchases. He took the tapes to the local TV stations and they aired them on the news. Someone recognized the thief and called the police.

To the victim’s surprise and horror, it was a clinical lab technician at the cancer clinic where he received his treatments. Because the victim’s information had been stolen from his health records, the case was given to the federal government, Office of Civil Rights, for prosecution.

A couple of weeks ago, the lab technician became the first person ever to be convicted and punished for a criminal violation of the Health Insurance Portability and Accountability Act of 1996. He will have to pay restitution for the things he stole, serve 10 to 16 months in prison, and pay unspecified damages to the victim.

This person might very well have gotten away with this had he not been a health care provider. The Office of Civil Rights was more than willing to devote the resources to prosecuting this criminal, when the State of Washington might not.

HIPAA has teeth, and they are sharp. This person could have been sentenced to as much as ten years in prison and could have been fined one quarter of a million dollars.

Obviously, we’re not here to discuss criminal behavior. But it does exist and HIPAA was written to deal with it.

More often, we will be faced with HIPAA violations that happen because of inattention to details or lack of knowledge. Make no mistake, they are still violations and carry penalties. The penalties are monetary in nature, and the fines can range from one hundred dollars to one hundred thousand dollars. You need to understand what constitutes a violation and how to avoid those circumstances.

HIPAA is a huge law. It was conceived by Senators Kennedy and Kassebaum, and originally written to protect Americans from having their health information used against them in employment decisions, reform medical liability, reduce fraud and abuse, and allow workers to keep their health insurance and levels of coverage when they move from job to job or retire.

What we have managed to focus on is a relatively small part of the whole act. It is known as Title II, Subtitle F, Part C, Administrative Simplification. You can rest assured that when the government talks about administrative simplification, they are not trying to simplify your administrative tasks. I'm not even sure that simplification is the right word to use. All the talk about administrative simplification got started because most of us who were involved in medical billing and health insurance wanted to use electronic transactions to cut the overhead associated with paperwork. By 1996 most people had heard of Electronic Data Interchange (EDI). It was common in manufacturing, retail, and banking. We were sure that it would work for health care as well. And with the growth of the internet we had the "information superhighway" waiting to be used. As soon as we said the word 'internet', the security flags went up everywhere. Everyone instantly became a believer of all the urban legends. As we all know, the internet is wide open and anyone with a computer can see anything about anybody, anytime. Please believe me when I tell you that after thirty five years in the information industry, I can more easily break into a post office and steal paper claims on their way to the insurance company than I can catch an electronic one on the internet. Nevertheless, HIPAA was expanded to include assurances for the protection of electronic data, and we were blessed with the Privacy Standard. Those that wrote the Privacy Standard liked it so much that after it was done, they decided to make it apply to all communication of health information, not just that done on the internet. And that is mostly what we will talk about today.

You should be aware as either employers or employees, you have many rights and responsibilities under HIPAA that apply regardless of the fact that you happen to be in the Healthcare Industry. For instance, if you work for a doctor, and also are a patient of that doctor, the doctor may not use anything in your health record to make employment based decisions about you unless you give him permission to do so. If you are a doctor or hospital who offers employees a health insurance plan, you cannot deny new employees coverage of preexisting conditions as long as they were covered for them under a previous employer's plan.

But you want to know what's going to get you fined or put in jail for doing your job everyday. So that's what we'll talk about. At the heart of the matter is the patient's right to privacy, and he or she has the final say about what his or her protected health information (PHI) will be used for.

You must obtain specific patient permission, in the form of a written authorization, for every disclosure of protected health information, and by specific I mean what is being disclosed, where it is going, what it will be used for and how long it will be used. This is an 'opt-in' situation. I can best explain that by mentioning another recent piece of federal legislation you have all been affected by, whether or not you have noticed, called the Gramm Leach Bliley Act (GLB). This law required all financial institutions such as banks and credit card companies to inform you in writing of how they use your personal information, such as your income level, marital status, number of dependents, etc. This notification was usually done in the form of a mass mailing which most of us discarded as junk mail. If you did happen to open one, the print was probably

too small to read, so you tossed it anyway. And that is exactly what the sender intended for you to do. Because GLB is an 'opt-out' situation. Unless you reply to the sender in writing asking them to take your information out of their system, they are free to continue doing whatever they were doing before, such as selling you to a telemarketing company. HIPAA, being an 'opt-in' situation, means you, as the health care provider must immediately stop using all patient information until you ask the patient for authorization in writing each and every time you want to do anything with protected health information. There is no blanket authorization. Even if a patient wanted to sign such a document, it would not be valid under the law.

There are three exceptions to this, however. And they are fairly significant exceptions, since they make up about 95% of your daily work. Uses and disclosures that do not require patient permission are those used for Treatment, Payment, and Healthcare Operations (TPO). All covered entities should have published a Notice of Privacy Practices as required, and provided each patient with a copy. In that notice was a sentence saying that patient information would be used for rendering treatment, to receive payment for that treatment, and to conduct healthcare operations. Many providers feared that if a patient refused to sign for the Notice, thereby giving their consent, they could not render care. HIPAA was changed to eliminate this. If a patient obtains healthcare from a provider, that provider may use the patient's information, without any form of permission, for treatment purposes, to obtain payment for that treatment, and within the practice for healthcare operations. Patient consent is a voluntary matter and may be handled in any way the covered entity wishes.

Even though most uses and disclosures fall into one of these three categories, there are still some limitations as to how those disclosures should be made.

The first term that everyone should be aware of is the 'Minimum Necessary Standard'. The HIPAA Privacy Rule requires a covered entity to make reasonable efforts to limit use, disclosure of, and requests for protected health information to the minimum necessary to accomplish the intended purpose. You must make your own assessment of what protected health information is reasonably necessary for a particular purpose, given the characteristics of your business and workforce, and to implement policies and procedures accordingly. This is not an absolute standard and covered entities need not limit information uses or disclosures to those that are absolutely needed to serve the purpose. Rather this is a reasonableness standard that calls for an approach consistent with the best practices and guidelines already used by many providers and plans today to limit the unnecessary sharing of medical information.

The minimum necessary standard requires covered entities to evaluate their practices and enhance protections as needed to limit unnecessary or inappropriate access to protected health information. Professional judgment is an equal partner with this standard. Therefore, it is expected that covered entities will utilize the input of prudent professionals involved in health care activities when developing policies and procedures that appropriately limit access to personal health information without sacrificing the quality of health care.

The next term that you must know is 'Incidental Use and Disclosure'. The HIPAA Privacy Rule does not require that all risk of incidental use or disclosure be eliminated to satisfy its standards. Rather, the Rule requires only that covered entities implement reasonable safeguards to limit

incidental uses or disclosures. I am always asked how can health care providers engage in confidential conversations with other providers or with patients if there is a possibility that they could be overheard? Many providers thought that they would be required to build private, soundproof consultation rooms, and ban all conversation in waiting rooms. The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. We must ensure that providers' primary consideration is the appropriate treatment of their patients. Oral communications often must occur freely and quickly in treatment settings. Thus, covered entities are free to engage in communications as required for quick, effective, and high quality health care. Overheard communications in these settings may be unavoidable and these are allowable incidental disclosures.

For example, the following are permissible under the Privacy Rule, if reasonable precautions are taken to minimize the chance of incidental disclosures to others who may be nearby:

- Health care staff may orally coordinate services at hospital nursing stations.
- Nurses or other health care professionals may discuss a patient's condition over the phone with the patient, a provider, or a family member.
- A health care professional may discuss lab test results with a patient or other provider in a joint treatment area.
- A physician may discuss a patients' condition or treatment regimen in the patient's semi-private room.
- Health care professionals may discuss a patient's condition during training rounds in an academic or training institution.
- A pharmacist may discuss a prescription with a patient over the pharmacy counter, or with a physician or the patient over the phone.

In these circumstances, reasonable precautions could include using lowered voices or talking apart from others when sharing protected health information. It would be unreasonable to shout across a room when you could easily walk to the person and speak in a lowered voice. However, in an emergency situation, in a loud emergency room, or where a patient is hearing impaired, such precautions may not be practicable. Covered entities are free to engage in communications as required for quick, effective, and high quality health care.

The question that comes up the most is: "May physician's offices or pharmacists leave messages for patients at their homes, either on an answering machine or with a family member, to remind them of appointments or to inform them that a prescription is ready? May providers continue to mail appointment or prescription refill reminders to patients' homes?"

You are permitted to communicate with patients regarding their health care. This includes communicating with patients at their homes, whether through the mail or by phone or in some other manner. In addition, the Rule does not prohibit covered entities from leaving messages for

patients on their answering machines. However, to reasonably safeguard the individual's privacy, covered entities should take care to limit the amount of information disclosed on the answering machine. For example, a covered entity might want to consider leaving only its name and number and other information necessary to confirm an appointment, or ask the individual to call back.

A covered entity also may leave a message with a family member or other person who answers the phone when the patient is not home. You are permitted to disclose limited information to family members, friends, or other persons regarding an individual's care, even when the individual is not present. However, covered entities should use professional judgment to assure that such disclosures are in the best interest of the individual and limit the information disclosed.

In situations where a patient has requested that the covered entity communicate with him in a confidential manner, such as by alternative means or at an alternative location, the covered entity must accommodate that request, if reasonable. For example, a request to receive mailings from the covered entity in a closed envelope rather than by postcard is a reasonable request that should be accommodated. Similarly, a request to receive mail from the covered entity at a post office box rather than at home, or to receive calls at the office rather than at home are also considered to be reasonable requests, absent extenuating circumstances. What kind of extenuating circumstance? A patient who works the graveyard shift might ask to be contacted only at work from midnight to 6:00 AM. This would not be possible if your practice was closed during those hours, and you could refuse the request.

Another common problem arises from a parent's right to see their child's medical records. In these cases, a parent is considered a personal representative as defined by HIPAA, and is entitled to access all healthcare information about the child, as long as local State law permits it. There are always some exceptions. If the State allows the minor to consent to care without adult permission, or if the treatment is court ordered, then the provider may withhold information from the parents. As is the case with respect to all personal representatives under the Privacy Rule, a provider may choose not to treat a parent as a personal representative when the provider reasonably believes, in his or her professional judgment, that the child has been or may be subjected to domestic violence, abuse or neglect, or that treating the parent as the child's personal representative could endanger the child. This leads to the question of personal representatives in general, and how they should be treated in regards to HIPAA.

State or other law determines who is authorized to act on an individual's behalf, thus the Privacy Rule does not address how personal representatives should be identified. Covered entities should continue to identify personal representatives the same way they have in the past. However, the HIPAA Privacy Rule does require covered entities to verify a personal representative's authority. Once a personal representative has been identified, he or she is to be treated the same as the patient in terms of disclosure of information without authorization.

If protected health information is to be used and disclosed for purposes other than treatment, payment and health care operations, written authorization must be obtained in advance. Again, there are more exceptions. Government agencies such as the Center for Disease Control, local Health Departments and law enforcement agencies may access information without prior

authorization from the patient if they are permitted to do so by state and federal law, or if they have a court order requiring the disclosure. However, there is still some work required on your part as covered entities. You must maintain a disclosure log for every patient. Each time protected health information is used or disclosed, an entry must be made in the log, and this applies whether the patient has given his authorization or not. Remember, this does not apply to treatment, payment and healthcare operations, not does it apply to incidental disclosures, which we discussed earlier.

As you can see, there are a lot of forms that need to be completed and maintained to satisfy HIPAA. I recommend to everyone who maintains a patient chart that a section be devoted to HIPAA and all applicable forms be kept in that section. And just in case you have forgotten some of the required forms, I will list the most common ones:

Acknowledgement of Receipt of Notice of Privacy Practices – this is optional now, but if the patient signs one, you should keep it in the record.

Request for Limitations and Restrictions of Protected Health Information – you may refuse unreasonable requests, but if you agree, then you must abide by your agreement. This form may be one of the most important to keep near the front of the chart, and should be checked every time you contact the patient to make sure you are not violating restrictions you agreed to.

Patient Authorization for Use or Disclosure of Protected Health Information – remember that it must be specific including an expiration date.

Request to Inspect and Copy Protected Health Information – if copies are made it is imperative that you record where and when, because you now have lost control of the information that was copied. It could be disclosed by the patient in some other way and you must be able to prove the patient had a copy. You may charge for the service and the doctor may refuse to allow the inspection if he believes it is not in the patient's best interests. For instance, psychotherapy notes are rarely allowed to be inspected by the patient.

Request for Correction/Amendment of Protected Health Information – my personal favorite since it seems unlikely a patient will notice a mistake in his health record unless some gross error has occurred. Again, the physician must approve the correction and may refuse if he disagrees with the patient.

Request for Accounting of Disclosures – a copy of which can be requested by each patient once per year at no charge. More frequent requests are chargeable.

Patient Complaint Form – this is the one we hope to never see. Your HIPAA Privacy Officer, which you all must have, should try to resolve the matter first. If the patient is still not satisfied, he may forward his complaint to the Office of Civil Rights. They will review the complaint and contact the practice if they believe a violation has occurred.

In addition to these forms which you must create, there are the court orders, health department requests, communicable disease reports, insurance company releases and others that will come

from outside entities. In order to be in complete compliance, all such forms must be included in the patient record.

By the way, there are other ways you can violate HIPAA regulations besides the Privacy Rule. It is a violation to transmit a nonstandard electronic transaction, such as an insurance claim. If your billing computer software is able to send transactions directly to an insurance company, you should be sure that the transactions have been certified by an outside agency. This whole issue can be avoided by using a health insurance claims clearinghouse. HIPAA was very careful to make the clearinghouse the loophole for standard electronic transactions. You can send your transactions to a clearinghouse in any format they will accept, and it is up to them to make them HIPAA compliant before sending them on to the insurance company.

And it is not over yet. Beginning in April of 2005, you will be required to comply with the Security Rule of HIPAA. If you have not started preparing for this, you are late. The law requires you to do a complete risk analysis of your organization, determine everywhere there might be a security issue, and develop a plan to prevent and/or recover from any such breach. This includes everything from a disgruntled employee damaging files to a hurricane wiping out your entire office. Patient information must be protected and maintained.

So as you can see, this is a very large set of regulations which you must comply with. The good news is that nearly everyone I work with is now and always has been HIPAA compliant. Very few doctors were in the habit of passing out patient information to anyone who asked for it. But what most practices were not doing is the documentation. HIPAA compliance is all about documentation. You should have signed Workforce Confidentiality Agreements for each employee in the practice, including the doctors. You should have proof of training on HIPAA Privacy and Confidentiality for everyone, with annual updates, including the doctors. You should have a HIPAA Policies and Procedures Manual which includes all the necessary forms and how to complete them. Having all this documentation will greatly reduce the chance of being cited for a violation. Not having it is actually a violation.

I want to leave you with a great resource. It is the department of Health and Human Services website, www.hhs.gov/ocr/hipaa. This can be your one stop for questions regarding HIPAA. On the frequently asked questions page, you can search by topic or keyword and if you don't find an answer, you can suggest the question and they will reply. It is the most current, most authoritative source of HIPAA information, and it is free. And if you wish to contact me, my email address is lastickney@hcrnet.com.

Thank you very much.