Providers

Legislative History

The law was originally known as the Kennedy-Kassebaum Act and was enacted in 1996 under the name "Health Insurance Portability and Accountability Act." The original intent of the law was to provide portability of healthcare insurance so that people with illnesses were not trapped in jobs, unable to get insurance if they changed jobs or had a brief period of unemployment. This group of reforms is already in effect. Tacked onto this was an "accountability" provision, a reaction to the belief that fraud and abuse is an expensive cost in American healthcare; these provisions have also been enacted.

Administrative Simplification

The Administrative Simplification section of the legislation is what is getting all the attention now; it's still an open issue. When the HIPAA law was being debated, many in the industry lobbied for a cost-saving provision. The hope was that costs could be reduced by setting standards for electronic transmission and collection of data. This would allow all participants in healthcare transactions to smoothly exchange electronic data. These electronic transactions should ultimately lead to lower costs. HIPAA's administrative simplification provisions are aimed at achieving that goal. An undoubtedly valuable idea—to agree on electronic standards—has been bogged down by concerns about the privacy and security of patient health data once it enters the world of electronic transactions. Six years after the passage of the HIPAA law, we are still working out the difficult issues of:

- Establishing electronic standards.
- Guaranteeing that electronic data is secure.
- Guaranteeing that all who touch healthcare data respect its privacy.

These are the issues we still confront today
The decisions are political, but the pain is economic and operational. The electronic transaction standards are difficult to agree on, and it is painful to force all participants in the system to invest in new hardware and software. Privacy standards are needed, but they introduce a new administrative layer that could slow down our processes. Security standards and software are needed, but they demand investment, and they too will slow down what we do. It will be painful to get from here to there.

Although the ideas behind HIPAA make sense, it is a lot for us to bite off and chew. We do hope that, once we agree on standards and establish healthcare data safely in electronic networks, the entire system will benefit greatly. Administrative costs will come down, and more importantly, the quality of care will improve with computerized records and decision support software. Getting there may be painful, but the political environment is committed to it…so buckle up. HIPAA is the latest in a century of efforts by the federal government to shape the healthcare system. Among these efforts, HIPAA is one of the most dramatic.

The HIPAA law will make far-reaching changes to the healthcare landscape. Organizations that are unable to effectively manage private and secure electronic health information will not survive and will be absorbed by organizations that can do so. The healthcare landscape will be different in five years, with clear HIPAA winners and HIPAA losers.

To an institutional physician, privacy training is intended to teach basic principles of privacy protection and create an awareness of the problem. Learning how other members of your organization handle privacy and security issues will help you to better understand the environment. HIPAA makes few specific requirements of physicians. You will need to understand and work with the general mechanisms of privacy protection. While many others in the hospital will be deeply affected by the privacy regulations, the impact to you will not be as great. As a physician, when your use of healthcare information is for direct patient care, you will continue to have access to all the patient information you need. However, other employees will not.

As a physician, you'll be subject to the **verify requester** rule. This means that, when requesting patient information, you will be required to verify who you are. The law gives latitude to organizations to decide how to do this, so be prepared for a variety of approaches. Other members of the healthcare team will be subject to the **minimum necessary** rule. This means that they will only be able to access the minimum amount of information necessary to do their jobs. As a physician you too will be subject to this rule, to a certain degree. The implementation of this rule will vary by institution.
There will be few specific requirements for you. You'll be asked to make an extra effort to safeguard privacy, such as keeping your voice low in crowded areas. When discussing cases where others can overhear, you must be careful not to include identifying information. When dictating, you must take precautions not to let unauthorized people hear identifying details about your patients. The same applies to

telephone calls. The law does not forbid conversations in open areas where others can overhear, but it does require you to take reasonable precautions to protect the privacy of your patients. When interviewing a patient in a shared environment, such as a double hospital room or a crowded ER, remember to keep your voice low and remember that others are listening. The law lays broad guidelines for the types of privacy practices required but does not specify details of implementation. It is left to the specific organizations to actually enact the requirements of the law by developing policies, procedures, and systems. If you practice in more than one institution, you will notice a variety of mechanisms for the practice of privacy protection.

The spirit of the law is to not put any barriers between you and the patients you are treating. In general, the law respects both the need for a physician to have access to all information in an efficient manner and the need to discuss cases with the patient and other caregivers. Still, the minimum necessary disclosure rule applies. The law asks that you use your judgment to not disclose any private information that is not needed for the job at hand.

Questions and Answers

Q: Does the HIPAA law mean it's going to be harder for me to get the information I need?
A: Yes and no. The law was specifically written to require that health information be readily available to those who need it for patient care. Practically speaking, if you encounter delays or significant barriers, these are problems in your system and problems with the start-up of new processes that must be worked out.

Q: Will my access to patient information be restricted?
A: You will experience the minor barrier of being asked to authenticate yourself in a way that you have not had to do before. Once you learn how to do this, it should be easy. And once you are given access, you should always expect to be given everything you need to care for the patient.

Q: Are there any new forms for me to fill out or any new paperwork with HIPAA?
A: No, there shouldn't be for the physician in clinical practice. If you are managing the business of a practice, however, you must know about the Notice of Privacy Practices, authorization forms, and some other documents.

Two areas of importance to physicians beyond usual protection of privacy:

- **Verifying, or authenticating, yourself**. In many situations, you will now be asked to prove who you are. You may also be asked to prove that you have a relationship with the patient that requires you to see his or her information. You will learn from your organization how to verify yourself. Once you get familiar with this process and become creative about other back-up methods to prove your identity, it should be easy. A physician number, a medical license, a call back to your office—there are many ways by which you can prove who you are.
- **Using and disclosing health information**. You must also know the rules about using and disclosing health information. You are probably already cautious about talking to employers or insurance companies without your patient's consent. Talking to family members about your patient will now require that you be sure that the patient does not object to this. As you've seen, the patient's decision to allow family disclosures should be documented and recorded. By doing this, you can refer to this record if you have a question and the patient is not available to ask directly. You can no longer assume a patient won't mind family disclosures.

Pharmaceutical and Device Companies

The HIPAA law makes it very clear that we can't share our patient's health information without a written authorization from them. Physicians have control over a valuable asset: information about patients contained in medical records. Pharmaceutical and medical device companies need this information for marketing and clinical trials. We physicians need to protect this information at all times and only share it with pharmaceutical and medical device representatives when patients have provided their written authorization. In the past, we have been cautious about these practices, and we have usually had the best intentions — to enroll a patient in a clinical trial or to provide access to information about new products. Now, however, with the HIPAA law, there's no gray area; any time a physician tells a pharmaceutical or device company about a patient, the physician must have that patient's specific authorization for this disclosure.

Q: I understand that the patient has to give authorization each time I disclose PHI. But there are times when I am inserting a new pacemaker that I allow the pacemaker rep to scrub in with me and observe. He doesn't try marketing to this patient. Is that okay?
A: It's not okay. If the device representative is present in the room, then the representative has access to the patient's protected health information. The representative can only be present with a specific authorization from the patient. Anything else is breaking the law.

Q: What if a pharmaceutical company rep wants a list of my patients that might be possible candidates for a new, revolutionary drug? They say they will only use the list to send authorization requests to the patients for enrollment in a study.
A: They certainly can't be enrolled directly in drug trials, and a drug company can't send marketing materials to them. You must first discuss this information with your patient and obtain the patient's signed authorization for you to be able to notify the drug company about the patient and to share any of the patient's PHI.

Disclosing PHI for Research

Accessing a list of patient names to send them authorization forms for research could be acceptable if it is considered "preparatory to research". But it would only be "preparatory to research" if the PHI were not removed from the hospital facility; also, the researcher (the pharmaceutical company) would have to represent to the hospital that the PHI was necessary for the research, and that the PHI would not be used for anything other than research (i.e. marketing).

Changes in Work Habits

Physicians are busy people, and often perform multiple tasks simultaneously. While we have always made an effort to respect privacy, there are times when our efforts to juggle tasks may result in violating a patient's privacy. Leaving charts, encounter forms, medical records or any other form of written PHI out where other patients or members of the public can see them exposes us to liability. Answering pages, talking to other healthcare providers, or handling phone calls from insurers should be performed in a manner to ensure that the PHI discussed is treated with complete privacy. Discussing a patient's PHI while in the presence of other patients or people who do not have a right to that information is always a hazardous practice. Even leaving patient information out, such as x-rays or laboratory slips, presenting interesting cases at Grand Rounds or leaving a computer screen exposed after looking up a patient's laboratory values exposes us to the risk of a privacy violation.

Q: All the charts on the desk where I complete my dictations are covered. Sometimes when my office gets busy or I have to privately confer with my patients, I have them wait in my office. I even put magazines in the room for them. Am I okay?
A: You're really exposed there. Your patients' charts, often including their sexual or psychiatric histories, are on your desk and are easily browsed by any patient who waits in your office unattended. You could have serious trouble if another patient discovered one of your patients' histories or someone unauthorized to view that information. You, your office manager or your nurse need to perform an "environmental assessment" of your office to ensure that all written or computer accessed PHI is secure and not capable of being accessed by people not directly involved in the patient's care.

Q: Taking calls from physicians — I can't avoid that. I know the other patients can hear me talk, but I never identify the cases I'm speaking about. Surely I can do that?
A: In theory, it's possible that you could protect your patient's information in these calls. But in practice, it's extremely risky. Any detail that you divulge that would identify one of your patients to another patient exposes you to liability under HIPAA. In both your consultations and day-to-day conversations you must always remember to guard a patient's PHI. You never want to speak about one patient within earshot of another patient or someone not authorized to hear that information.

Q: I've started answering some of my patients' questions by email. Is that a problem?
A: You'll need to take reasonable steps to ensure you have the patient's permission to communicate PHI by email, and to verify the correct email address with the patient.

Q: What if I take all of these reasonable steps, but I find out someone intercepted an email about one of my patients?
A: That would be an incidental disclosure, so you wouldn't be breaking the law -- but you should report the incident to your Privacy Officer.

Disclosures to Family and Friends

There are now rules to protect even family discussions with privacy safeguards. Patients now have the right to opt out of family discussions by telling us at the time of first contact, or any time thereafter, what their own personal ground rules are for disclosing health information to family members and close friends. The patient's opt-out decisions are recorded in the healthcare system so that all caregivers can keep this information in mind when interacting with family of the patient. As a physician, family members frequently ask you for clinical information on your patients, and you'll need to know how your patient wants you to respond to these requests.

Q: I practice in several different environments, and it's not clear to me where to find this information about the patient's opt out decisions. Why can't I just use my judgment?
A: The law states clearly that you are to use your professional judgment. If you are unable or unsure where to find the patient's opt out decisions, just check with the patient directly. A simple question, such as, "Do you mind if I tell your wife about your condition?" is sufficient. The idea is to just let the patient object and let them state the ground rules for family disclosures.

Family Discussion and Opt-Out

Opt-out applies to disclosures of PHI to the family and friends involved in a patient's healthcare and to the use of information in facility directories.

The patient has the opportunity to refuse, or opt out of, this type of disclosure.

The law says that you can make information disclosures to family, close friends, or personal friends if you can reasonably infer from the circumstances that the individual would not object to the disclosure — so, in the end, use good judgment.

Minors can present a more complicated privacy problem. The HIPAA regulations defer to all state laws regarding the disclosure of a minor's PHI, so you must know the rules for your state

The Minor

The minor has the authority to act as his or her own individual in any of the following situations:

- If the minor is allowed by state law to consent to the healthcare service, has consented, and has not designated a personal representative.
- If the minor may receive the healthcare service by law without consent.
- If the parent or guardian consents to agreement of confidentiality between the minor regarding health information and us.

Protected Health Information

Use this easy decision device to determine if medical information qualifies as PHI.

1. Does the information identify an individual or is there a reasonable basis to believe that the information can be used to identify the individual? *If yes, proceed to #2.*
2. Does the information relate to the past, present, or future physical or mental health or condition of an individual or the provision of health care to that individual or the past present or future payment for the provision of health care to an individual? *If yes, proceed to #3.*
3. Was the information created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse? *If yes, proceed to #4.*
4. Is the information education records or post-secondary student medical records that are covered in the Family Educational Right and Privacy Act or 20 USC 1232g(a)(4)(B)(iv), or is the information employment records held by a covered entity in its role as an employer?

Only health information that identifies an individual is subject to the HIPAA privacy rule. Health information that could not be reasonably used to identify an individual is not subject to the privacy rule and can be freely disclosed.

Health information can be "de-identified" by removing all of the following identifiers regarding the individual, relatives, employers, or household members:

- Names
- Geographic subdivisions
- All elements of dates
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account Numbers
- Certificate/license numbers
- Health plan beneficiary numbers
- Account numbers
- Vehicle identifiers
- Device identifiers and serial numbers
- Web Universal Resource Locator (URL)
- Internet protocol (IP) address number
- Biometric identifiers
- Full-face photographic images
- Any other unique identifying number, characteristic or code

Verifying the Requester/Minimum Disclosure

Patients have been notified that we will use their information in day-to-day business.
But we have to be **careful** with people's health information. The two key principles of being careful with health information are:

- Verifying the requester
- Disclosing only minimum necessary information

Verify Requester

To verify the requester we must verify both the **identity** and the **authority** of the person requesting information.

Verify Identity
There are many ways to verify that people are who they say they are:

- Ask for a birth date or social security number
- Ask for the mother's maiden name or some other unique information
- Check a physical signature against a known one on file, or
- Make a call back to a known number

Verify Authority
Once you know who the requester is, verify that he or she has the right to access this information.

Routine request from employees you know in your own organization are usually OK.

You must verify both the identity and the authority of the requester to be sure you can disclose protected health information.
Even after we have verified the requester, we must disclose **minimum necessary information** to take care of PHI.
Once you are comfortable with the requester, give out only what the person really needs to know. Our co-workers will usually only ask for what they need. Unusual requests from individuals you don't know are risky. Limit the information you give out—no more than **exactly** what they are authorized to receive!

We need to be careful with people's health information. People expect that we will protect their information from anyone who does not need to know it, even our own employees.

Our organization has specific policies and procedures to help you decide how to make or request disclosures in your daily work. Be sure you know the policies that apply to you.

If you are in doubt, or something doesn't feel right, ASK! You must go to your supervisor or privacy officer for help.

Damage Control

Our organization is committed to making sure that individuals are not harmed by the unauthorized disclosure of their protected health information.

What should you do if you learn that private health information has been released outside of routine business functions, without authorization?

Tell your supervisor, or the privacy officer! We have a duty to MITIGATE THE EFFECTS of unauthorized release.

This is to certify that I, _____ have read and understand all policies and guidelines governing the HIPAA regulation.

_____ _____

Signature Date