1. Physicians who transmit health information in electronic form for billing or transferring funds for payment are subject to all of the rules and penalties of HIPAA.

2. Disclosure of personal health information (PHI) is appropriate if:
   (a) given to the patient;
   (b) given to anyone specifically authorized by the patient;
   (c) required by law; or
   (d) used for purposes of treatment, payment, or in usual business operations.

3. Physician disclosures of PHI to hospital quality assurance, risk management, institutional research, and ethics review committees are appropriate.

4. Beware of disclosure of PHI to patients’ family members and “representatives”:
   (a) know the recipient of the PHI;
   (b) ask the patient to specifically authorize who can receive PHI;
   (c) if the patient cannot make decisions, consult advance directives or ask the family to appoint a spokesperson;
   (d) document the process in the chart.

5. Use caution when sharing PHI with health care entities not in the usual course of your business operations, treatment, or billing.

6. Never “lend” your EHR password to anyone else, especially your family members, secretary, or nurse.

7. Close all EHR accounts before leaving a terminal or PDA!

The physician–patient relationship creates an obligation on the part of the physician to protect certain confidential patient information. Cultural assumptions about the relationship between the physician and the patient create a duty on the part of the physician to keep information private. Improper disclosure of that information, or breach of that duty, should necessitate some punishment of the physician and some compensation to the patient. The concept seems self-evident. This chapter will differentiate between commonly cited assumptions, advisory guidelines, and binding laws that populate the landscape of physician disclosure of confidential information.
CASE PRESENTATION

Case A. On busy medical rounds in the Intensive Care Unit (ICU) an attending physician stops in to see her patient with advanced dementia and aspiration pneumonia on a mechanical ventilator. The physician knows that the patient’s dedicated daughter is the power of attorney for health care decision making and assumes that there is a happy family situation. While in the ICU, the physician is notified of a phone call from the patient’s son in a distant state. The physician explains the patient’s dire situation. The son asks the physician to explain the medical details to the “family” attorney on speakerphone so that the son can begin to “tide up” his dad’s affairs. The physician also faxes the lawyer some medical records. Later that day, the patient’s daughter calls the physician in an irate state. She explains that her estranged brother filed papers alleging that she has committed elder abuse. He is seeking the appointment of a guardian to strip her of her status as power of attorney and that she may no longer be able to access her father’s sizeable estate to pay for his ongoing care at home. She states that her brother is manipulative and has a long history of attempts to access their father’s estate for his own use.

Case B. A busy private, multi-specialty group has been recruited by a local hospital system to have its paper medical records merged into the hospital’s comprehensive electronic medical health (EHR) system. The relationship is mutually beneficial to the hospital and the group. The hospital and its many specialty centers gain increased accessibility, uniformity, and continuity of records for thousands of patients from a new referral source. The private multi-specialty group is able to free up space and reduce document expenses by going “paperless,” and in doing so convert a chart storage room into a new lab. The cost of computerizing the medical records is paid by the hospital system. Three months after the merger of medical records, a patient of the multi-specialty group learns that her private records (formerly kept in paper form in the group’s locked offices) were accessed electronically by a medical student rotating at the hospital. The medical student had no legitimate, professional reason to access the confidential information, but has spread sensitive psychiatric and obstetric information in the community. The patient is outraged and wonders why her confidential medical information was converted into electronic records without her permission and then shared with a hospital system, thousands of hospital employees, and hundreds of caregivers with whom she has no professional relationship. She asserts that her records were shared without her permission and done so for the financial benefit of her former medical group and the hospital system.

ISSUES

Introduction

Physician stewardship of patient confidential information is not as clearly articulated in the law as many think.
First, new federal regulation known as the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") creates federal civil monetary and criminal penalties for improper disclosure of confidential patient information, but does so without giving patients rights to personally sue a doctor for misuse of confidential information. Under HIPAA, patients make complaints of improper disclosure of confidential information to the Office of Civil Rights of the Department of Health and Human Services and proceedings are brought in administrative hearing.

Second, prior to HIPAA, physician responsibilities for protecting confidential patient information were explicitly codified only in the ethical and professional standards of the profession and the language of state licensing acts. A cause of action in court to recover financially for losses caused by an improper disclosure must be grounded on less specific state common law theories of breach of confidence or invasion of privacy. Of course, myriad mandatory reporting laws make it obligatory for physicians to disclose certain confidential patient information to protect public health or prevent crimes. In those cases, there is no violation of professional standards or a breach of confidentiality cause of action.

Third, the legal concept of doctor–patient privilege needs to be differentiated from the topic discussed in this chapter. Legal actions are governed by rules of evidence that determine the admissibility or discoverability of certain information. Privilege refers to a class of information that is exempted from use in court. The right to exert privilege to prevent certain information from being used belongs in some instances to the person in possession of the information (physician) and in some instances to the person who is the subject of the information (patient). Specifically, the doctor–patient privilege never historically existed in English and American law. The privilege was created only later by state statutes. Today, however, there are many exceptions to statutory doctor–patient privilege stemming from mandatory reporting of public health information, in all matters pertaining to criminal cases, and in malpractice and workers compensation cases where the patient puts his medical condition into issue. Despite popular cultural assertions to the contrary, the concept of doctor–patient privilege is largely without legal viability.

Foundations of Physician Confidentiality

Thousands of years ago the original version of the Hippocratic Oath enunciated the physician’s duty to honor patient confidences, describing a breach of that duty as something shameful. Modern versions of the Hippocratic Oath, recited at medical school commencements everywhere, do not diminish the original oath’s emphasis on the duty of the physician to keep private the confidences of patients. If anything, the modern version elevates the importance of patient privacy by situating it in the paragraph that reminds physicians to save life, to be humble witnesses to death, and never “to play at God.”

The ancient Greeks no doubt understood that medical care was a societal good. Healing loved ones, prolonging life, and promoting a healthy community serve basic human desires and put to good use the technological and scientific advancements created by society. Both in ancient and modern times, medical care functions most successfully when the patient is assured of complete confidence on the part of the physician.
The inevitable vulnerability one feels when sharing both nakedness and illness is surely the most fundamental source of the need for physician confidence. Within the family relationship the sharing of nakedness and illness is accepted because there exists an automatic assumption of protection, selflessness, and love. Expert medical care, however, is provided to an enormous degree outside of the protections of the family structure. Only if one is guaranteed that their vulnerabilities are protected—body, behavior, and illness—can patients feel secure in divulging their most human conditions. Medical care and the benefits it imparts on society are optimized when patients are honest with their physicians. The guarantee that society holds the physician responsible for confidential stewardship of that private information is an absolute requisite for medicine to function and yield benefits to the community.

**Modern Restrictions and Penalties Involving Disclosure**

Explicit codification of the physician responsibility to protect the confidentiality of patient information is found in advisory, nonbinding form in the Hippocratic Oath and the AMA Principles of Medical Ethics. Violations of these principles carry no penalties as they are not enacted or judicially endorsed, and therefore do not carry the enforceable power of state or federal law. Each state, however, has enacted legislation defining the scope and licensing requirements for the practice of medicine. Some state laws may explicitly describe the physician responsibility to protect confidential patient information. Others like the Illinois Medical Practice Act of 1987 may specify examples of dishonorable physician conduct that warrant discipline, such as failure to “safeguard patient confidence and records within the constraints of the law.”

It is essential to understand that violation of these licensing or disciplinary regulations results in *professional penalties* to the physician who improperly discloses confidential patient information. These penalties range from formal letters of sanction to permanent revocation of medical licenses. Hospitals and health care systems can likewise restrict or revoke physician privileges to practice within their institution for improper disclosure or use of confidential patient information. These penalties can severely impact a physician’s reputation and ability to earn a living, but they do not carry criminal or civil penalties that would allow for financial awards for aggrieved patients or jail time for the physician.

In most states, patients who suffer damages as a result of physician disclosure or misuse of confidential information seek redress under the common law theories of breach of confidence and invasion of privacy. Since a universally accepted cultural expectation of confidentiality exists between physician and patient, the law implies a contractual obligation or duty of confidentiality in the physician–patient relationship. The breach of the duty to protect patient confidence results in damage to the patient. The patient can assert the right to have the damage redressed by bringing an action against the physician seeking a monetary reward to make the patient “whole” again. Such civil actions can occur simultaneously with professional disciplinary investigations by state medical licensing bodies.
Since the advent of HIPAA in 1996 there has been new federal attention paid to the issue of privacy of patient records and improper disclosure or misuse of confidential information. HIPAA applies to all health care providers, including physicians, who transmit health information in electronic form for billing or transferring funds for payment. Physicians who electronically transmit health information to Medicare for purposes of reimbursement are subject to the HIPAA rules. Employees of physicians who are subject to HIPAA regulation are themselves subject to the penalties laid out in HIPAA.

HIPAA creates civil monetary fines for improper disclosure of confidential patient information. For the purposes of HIPAA, confidential patient health information is regarded as individual identifiable patient health information—what the Act calls patient’s protected health information or PHI. The civil monetary fines created under HIPAA are imposed by the Office for Civil Rights of the Department of Health and Human Services. Investigation into covered entities, such as physicians, for improper disclosure of PHI is conducted by the Office of Civil Rights after a patient or other source makes a complaint. An action against the physician is then brought by the Office of Civil Rights in federal administrative court. The patient does not have an individual right to sue the physician or seek monetary award under HIPAA. Only disclosures of PHI that are not done knowingly are punishable by these civil penalties. The $100 civil penalty may be avoided in some circumstances where the disclosure is reasonable and cured within 30 days or when there was no knowledge that the conduct was a violation.

HIPAA also creates very severe criminal sanctions for knowing or purposeful disclosure of individually identifiable patient information. The Department of Justice enforces these criminal actions. Simple violations of PHI can result in fines up to $5000 and imprisonment in jail for a term of up to one year. Disclosures or misuse of PHI under false pretenses carries a fine of up to $100,000 and up to five years of imprisonment. Disclosure or misuse of PHI that is committed with the intent to sell or use the individually identifiable information for commercial advantage, gain, or malicious harm carries a fine up to $250,000 and up to ten years in prison. The criminal penalties under HIPAA apply to the employees of a physician practice, as well as to doctors and physician corporations. Moreover, the officers of a corporation whose employees improperly disclose PHI are subject to criminal penalties. In other words, the physician who operates a medical practice as a corporation is not protected from criminal penalties if an employee improperly discloses PHI.

Confidential Patient Information, PHI, and the Medical Record

The definition of confidential patient information is fluid and varies under different applications. For purpose of the common law actions of breach of confidentiality and invasion of privacy, a community standard would be applied by state courts to define the information shared within the physician–patient relationship that is expected and historically considered to be private. In other words, state courts would ask “What does the community and what does
prior case law accept as information that a physician should keep private?” Although not all states accept the invasion of privacy theory as a viable cause of action to seek recovery for improper physician disclosure of patient information, some invasion of privacy logic probably applies. To that end, no information that is publicly known would likely be considered confidential.

State medical boards and licensing agencies can be broader in the determination of what behavior constitutes improper physician use or disclosure of confidential patient information. Because state law widely empowers these bodies with the regulation of medical practice and physician conduct, there is great latitude afforded them to determine unethical or unprofessional behavior. Sanctions can vary from letters of censure to permanent revocation of license based on the severity of the misuse or disclosure.

Under HIPAA the definition of confidential patient information is laid out explicitly. As introduced earlier, the language of the Act refers to confidential patient information requiring physician protection as protected health information or PHI. The type of patient health information that physicians must protect from improper use or disclosure under HIPAA is information that is individually identifiable. In other words, HIPAA strictly protects health information that is particular to a patient and carries with it some identifying feature like name or address. Under HIPAA a physician is prohibited from disclosing PHI unless expressly authorized by the patient, required by law, or used for treatment, payment, or health care operations.

Disclosure of Electronic Health Records (EHR)

In April 2004 President Bush created the Office of the National Coordinator for Healthcare Information Technology (ONCHIT). The Office is responsible for coordinating nationwide implementation of Electronic Health Records (EHR) through various free-market incentive strategies and standardization programs. Long before 2004, physicians became aware of EHR systems as their hospitals, labs, and offices became computerized. One of the goals for the widespread application of these systems was improved data monitoring and sharing among appropriate parties.

The reality of the nationwide implementation of EHRs is the creation of new dilemmas for physicians to navigate, including new risks of improper disclosure of confidential patient information. The most important rule of thumb for avoiding improper disclosures in the world of EHR is to “sign out” of computerized charts when they are not actively being used. Open EHRs on doctors’ computers, at nursing stations, and on PDAs become violations of HIPAA as soon as someone other than the physician views them. While it can be argued that walking away from an EHR without closing the account is inadvertent, it might be argued that to do so was somehow a purposeful or knowing action or part of a pattern of willful physician neglect. If that argument is persuasive, the conduct is subject to the most severe criminal penalties under HIPAA. More dangerous still is the risk of malicious behavior perpetrated by someone accessing a physician’s unclosed electronic chart for purposes of order entry. While improper viewing of PHI can land a physician in jail, bogus or inexpert order entry can kill a patient. Another pitfall
that may justify criminal penalties under HIPAA includes the situation of a physician “lending” his EHR password to someone else to save time or increase productivity. In the rush to implement and incentivize EHR systems, there are many situations where physicians will be faced with difficult decisions about sharing PHI electronically.

**SURVIVAL STRATEGIES**

HIPAA suggests that protected health information (PHI) can be any kind of individually identifiable information: demographic, insurance, billing, or medical. This broad definition includes any information pertaining to a patient that carries with it an identifier unique to that patient. An EKG tracing that carries the patient’s social security number, a computer CD with a patient’s radiographic images and billing information, an email about therapies from a doctor to a patient with an email address on it, or a faxed page from a hospital chart with an imprinted date of birth and address all constitute PHI. Of course, the spoken word is not exempt from PHI. Telephone calls, voice mail, text messages, data recordings, conversations with medical students and nurses in the hospital, and face-to-face conversations on the street fall within the ambit of PHI and the protections of HIPAA.

The most difficult set of circumstances for the physician involves interpreting the situations where disclosure is proper or improper. PHI can always be shared with the patient. For many other situations, however, individually identifiable patient information should be shared only after the physician has obtained specific written patient authorization that includes the name of the recipient. Release of PHI to entities that may necessitate this level of specific authorization include those involved primarily in advertising, marketing, or internet business; employers and schools; attorneys seeking information without a subpoena or court order; other patients trying to contact your patient; and insurance companies that have never covered your patient or that are not involved in your efforts to collect a payment.

Sharing PHI with entities that are involved with billing, treatment, and health care operations should not cause a problem under the HIPAA rubric. These recipients of PHI include current insurers and billing clearinghouses; current and former treating physicians providing care or follow-up; hospital and health care businesses involved in continuing or outpatient care; pharmaceutical, medical device, and research companies tracking outcomes; hospital committees or employees involved in ethical or research review issues, disease reporting, quality review, risk management, or credentialing in the normal course of business; and government and police agencies seeking information under court order or for required mandatory purposes.

Areas that are unclear in regard to disclosure of PHI often involve two distinct situations. First, physicians often assume that their patients’ spouses and family members have the same selfless dedication and care for the patient’s wellbeing that the physician has. This of course is not axiomatic. Dysfunctional family dynamics and financial motivations often place family members, and surrogate decision makers, at odds with one another and the patient’s best interest. Disclosure of PHI in these situations can be fraught
with peril. It is best to ask the patient to specifically identify who is authorized to receive PHI, and if that is not possible, require the family as a whole to appoint a spokesperson for communication with the physician. Documenting the conversation in the chart and having a nurse or social worker witness the conversation is ideal. Only those family members or representatives whom the patient has identified as involved in their care or involved with their medical bills are automatically authorized to receive PHI.

Secondly, disclosure of PHI to health care organizations can be problematic when the motivation in disclosing the information is primarily economic and disclosure is not done in the usual course of operations, treatment, or billing. This situation often arises when physicians share access to PHI with health care entities interested in marketing or expanding their database of future patient-consumers. Even if a physician determines that disclosure of PHI is authorized because it pertains to some aspect of treatment, billing, or health care operations, HIPAA may still require that the patient receive advance notification of the intended use. As always, advanced and explicit patient authorization is the best plan for guaranteeing compliance with HIPAA requirements.

**FURTHER READING**


**REFERENCES**

5. Winn PA, Who is Subject to Criminal Prosecution under HIPAA? Available at www.abanet.org/health/01_interest_groups/01_ehealth.html