Privacy and Confidentiality 5

Creatas/Thinkstock

Learning Objectives

1. Differentiate between privacy and confidentiality in the legal and ethical context of health care practice.
2. Explore the legal and regulatory landscape affecting privacy and confidentiality in health care.
3. Analyze the ways in which health information technology can both protect and jeopardize patient privacy and confidentiality.

The necessity of protecting the privacy and confidentiality of patients is a fundamental value in both ethical and legal frameworks of American health care (Terry, 2003). Nonetheless, these concepts, for which there is little disagreement in theory, become increasingly fraught with controversies, confusion, and legal and ethical conflict as they are applied to the more practical everyday work of health care professionals (Terry, 2008).

In bioethics the conceptual underpinning of patient privacy and confidentiality is the principle of respect for persons and their autonomy. Tom Beauchamp and James Childress (2001) claim that privacy and confidentiality are "justified by rights of autonomous choice that are correlative to the obligations expressed in the principle of respect for autonomy" (p. 296). Charles Fried (1968) asserts that since "to respect, love, trust, feel affection for others and to regard ourselves as the objects of love, trust and affection is at the heart of our notion of ourselves as persons among persons," respecting a right to privacy is required for these values to flourish. If so, then respecting the privacy of patients is not simply an instrumental goal but is itself the manifestation of some of the intrinsically valuable and even ultimate ends of medicine (Terry, 2008). Although observing patient privacy and confidentiality was originally intended to promote an equitable exchange between health care practitioner and patient based on care, trust, and respect, it has been diluted to the means by which health care providers reduce harm and liability risks. Likewise, the laws and regulations that now govern privacy and confidentiality have become increasingly arcane, confusing, and insufficient to handle technological innovations. As a result, many people have begun to regard privacy and confidentiality as stumbling blocks to the progress of medicine.

In this chapter we will first differentiate between the concepts of *privacy* and *confidentiality*, which are often confused for one another. We will then take an in-depth look at the legal context surrounding the ethical notions of respecting a person's right to privacy and confidentiality. We will also consider the longer history of common-law approaches to these topics through case studies. The chapter concludes with a discussion about whether existing privacy and confidentiality laws and regulations are appropriate and adequately protect patients, given the rapid rate of innovation in biomedicine today. Then we will consider the future of ethical and legal health care management with regard to patient privacy and confidentiality.

5.1 Differentiation of Terms

In both clinical and legal contexts, the terms *privacy* and *confidentiality* are often used interchangeably, despite the fact that the two terms are not synonyms. This inconsistent, imprecise, and sometimes contradictory usage tends to cause confusion, especially when attempting to apply these ethical concepts to practical situations. It is therefore necessary to define and explain the differences between each of these terms.

Privacy

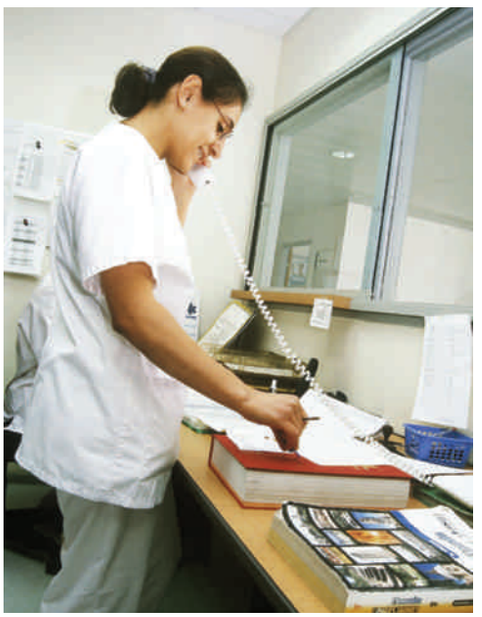
Privacy refers to an individual's expectation to keep or control access to his or her individual space as well as knowledge of certain information. What legally falls under this "zone of privacy" can vary depending on the jurisdiction or the context; the expectations of privacy can also vary by person, context, or culture. Access to intimate details and information is controlled by an individual's **right to privacy**. When allowing access to this private sphere, an individual is retaining control of

this right rather than waiving it. In legal terms, the right to privacy also encompasses the right to limit the interference of others when making personal and autonomous choices.

While in the broader sense privacy encompasses control over access to one's body or information, more subtle situations often require further precision of the term. Privacy law expert Anita Allen (1997) has identified four different types of privacy that exist in the realm of genetic medicine.

- **Informational privacy**: controlling access to personal information
- **Physical privacy**: limiting access to persons and intimate spaces
- **Decisional privacy**: limiting interference with personal decisions
- **Proprietary privacy**: retaining ownership interests in the person's body

All of these facets of privacy can readily be seen throughout modern health care. For example, one of the five requirements of informed consent we saw in Chapter 4 was the requirement of voluntariness. The requirement for voluntariness protects patients or research subjects from being coerced or unduly influenced in their decision making. This example represents the protection of what Allen (1997) regards as decisional privacy. Decisional privacy was discussed in Chapter 4 as an element of patient autonomy and consent. But note here the impact that a patient's religion may have on his or her health care decision. For example, the Jehovah's Witnesses position that a believer should not accept blood and Christian Scientists' limited acceptance of medical care led to case law establishing when an adult can refuse life-sustaining therapy as well as whether a parent can refuse such therapy for a child. Currently, Catholic opposition to abortion has been expressed in a series of cases challenging the Affordable Care Act's requirement that employers provide health coverage for abortion and birth control. This position, in conjunction with the merger of secular and Catholic hospitals, has led public interest groups and attorneys general to question, as part of their duty to oversee public charities, whether the merger will preserve adequate access to such services. Other examples include the numerous policies, guidelines, regulations, and laws that limit access to what has become known as a patient's **protected health information (PHI)** under the **Health Insurance Portability and Accountability Act (HIPAA)**. Protected health information encompasses the details a provider collects regarding the patient's condition, treatment, or payment that identify or have the potential to identify the patient. Caution and ease of application leads many to assume that any part of a patient's health record (including payment history) is likely to be considered PHI. The question then becomes less one of whether the information is protected as confidential and more one of whether the information can be disclosed. The trade-off in this question illustrates the difference between privacy and confidentiality.



Laurent/BSIP/SuperStock

Though closely related, the distinction between privacy and confidentiality is an important one. In the context of health care, privacy is a right of patients to control access to their person and information, whereas confidentiality is an obligation of health care providers to keep their patients' information secret.

Confidentiality

Confidentiality refers to the ethical and legal obligations to refrain from sharing information about other people without their authorization. In legal terms, these obligations result from the relationship or contractual obligation between those who are privy to the information and the rights holder. Respecting someone's right to privacy, on the other hand, is generally considered a social obligation, which does not require a specific contractual relationship or legal duty. Ethically speaking, the duty to keep others' private information secret is the appropriate response of someone who respects others as persons who are ends in themselves.

One popular translation of the Hippocratic oath from the National Library of Medicine (2012) requires physicians to vow:

> Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private.

The sentiment is mirrored in the Declaration of Geneva of 1948: "I will respect the secrets that are confided in me, even after the patient has died" (World Medical Association, 2013). The duty of patient confidentiality is stated in the American Medical Association's (1957) principles of medical ethics as follows: "A physician shall respect the rights of patients,. . . and shall safeguard patient competences within the constraints of law." The American Medical Association's (2001) ethical principles also reiterate:

> The patient has the right to confidentiality. The physician should not reveal confidential communications or information without the consent of the patient, unless provided for by law or by the need to protect the welfare of the individual or the public interest.

In clinical contexts, the American Medical Association's Declaration of Professional Responsibility (2001) vows:

> We, the members of the world community of physicians, solemnly commit ourselves to: . . . protect the privacy and confidentiality of those for whom we care and breach staff confidence only when keeping it would seriously threaten their health and safety or that of others.

Though rooted in the ethical principles of respect for persons, today the notion of confidentiality is more often justified with instrumental and utilitarian ends-means rationales. Terry (2008) identifies the current rationales for the need to observe confidentiality as "two co-dependent, practical imperatives: patients disclosing information to physicians to seek protection of their health and physicians respecting competences in order to encourage patients to disclose needed personal and medical information" (p. 16). Once considered a nearly absolute and inviolable duty, confidentiality is now a circumscribed protection, bending to a wide range of utilitarian exceptions. One such example is that health care providers can disclose protected health care information to another covered entity for the purpose of payment or, providing the information is limited, to credit reporting agencies (HIPAA Administrative Simplification, 2013).

As the American Medical Association's statement above notes, there is a need to maintain confidences unless disclosure is allowed by law or in cases in which an individual's welfare or the public interest are endangered. One such provision is embodied in case law, which requires a

psychiatrist, once he or she has formed a reasonable opinion that a patient has the intent and means to injure a specific person, to protect the potential victim by means of disclosure of the risk of harm (*Tarasoff v. Regents of University of California*, 1976). HIPAA treats such a disclosure as a permitted disclosure (HIPAA Administrative Simplification, 2013). There are additional HIPAA exceptions for disclosures required by child abuse and other public health reporting statutes.

Stop and Clarify: Privacy, Confidentiality, and the Right to Privacy

Privacy refers to an individual's expectation to keep or control access to his or her individual space as well as knowledge of certain information. It enables a person to limit who has access to his or her individual space or information, for what purposes, and for how long.

The right to privacy reflects an individual's legal right to control access to private information and the right to exclude others from intervening in personal decision making.

Once an institution or person is entrusted with otherwise private information or access, the duty of confidentiality restricts the disclosure of that information without permission or strictly defined necessity.

5.2 Legal and Regulatory Landscape Affecting Privacy and Confidentiality

American jurisprudence has long upheld a common law right of privacy. Note that the term *common law* refers to the body of law developed as the result of cases and extends back to the traditional, unwritten laws of England. In 1890 Supreme Court justices Samuel Warren and Louis Brandeis described the right of privacy as "the more general right of the individual to be let alone" (p. 205). Using Warren and Brandeis as support, in 1956 the court in *Housh v. Peth* described the common-law right to privacy:

1. The right to privacy is the right of a person to be let alone, be free from unwarranted publicity, and live without unwarranted interference by the public in matters with which the public is not necessarily concerned.
2. An actionable invasion of the right to privacy is the unwarranted appropriation or exploitation of one's personality, the publicizing of one's private affairs with which the public has no legitimate concern, or the wrongful intrusion into one's private activities in such a manner as to outrage or cause mental suffering, shame, or humiliation to a person of ordinary sensibilities.

In the 1976 case of *Estate of Berthiaume v. Pratt*, a commonly cited example of the strength of health privacy protections in America, the court found a physician liable for infringing on a dying cancer patient's right to privacy by taking unwanted photographs of the patient. The court argued that the physician had disrespected the patient's expectations to privacy by intruding in the patient's "physical or mental solitude or seclusion" (*Estate of Berthiaume v. Pratt*, 1976).

Despite the robust common law precedents that protect patients' rights to their privacy, case law construes the right to privacy in health care more narrowly. Hundreds of U.S. cases from the last few decades (see timeline of significant cases and legislation related to health care in the appendix) show how restrictive the right is. In the 1980 case *Knight v. Penobscot Bay Medical Center*,

the husband of one of the hospital's nurses dropped by to pick up his wife. Apparently noticing how bored the husband was as he waited, hospital employees allowed the husband to don a gown and intrude on a stranger's labor and delivery for entertainment. Although another patient had consented to the man's presence, the doctor thought this patient might have complications and so routed him instead to Mrs. Knight, who had not been consulted. If the law's rationale was based on the right of privacy, or the right to exclude those who have no business intruding on our most private spaces and moments, the result of this case—like that of *Berthiaum*—would be clear. But since the voyeur in the *Knight* case had not *intended* the intrusion, the court held that the plaintiff's lawsuit must fail (*Knight v. Penobscot Bay Medical Center*, 1980). Other cases show that in case law, the court balances the patient's right to privacy—i.e., to be left alone—with the public's need to know. Questions regularly arise concerning who can attend the birth of a baby—such as an unmarried father or surrogate parents—or whether a representative of a cardiac pacemaker or orthopedic device manufacturer can be present during surgery.

With the advent of computerized health records, the protections surrounding informational privacy have become more strictly defined. In addition to HIPAA, certain states have statutes that supplement HIPAA. For example, California's Confidentiality of Medical Information Act (California Civil Code, 2008) not only provides for the imposition of actual damages and attorneys' fee but also statutory damages. In 2008 University of California–Los Angeles (UCLA) Medical Center terminated 13 employees for inappropriately accessing Britney Spears's medical records. More recently, Cedars-Sinai Medical Center terminated five employees and a student research assistant for accessing the health records of Kim Kardashian. Note that the employees were terminated for merely *accessing* the records. Redisclosure was not required—and in fact, records of others such as family members are also protected from unauthorized access.

Although celebrity cases pose a potential reputational risk, there is significant monetary risk for patient information lost as the result of a security breach. Idaho State University, for example, recently paid $400,000 to settle the breach of unsecured electronic PHI of 17,500 individuals who were patients at a university clinic. WellPoint, a health plan, agreed to pay $1.7 million as the result of the disclosure of an application database containing the information of 612,402 individuals. As a result of the above, employers at every level of health care have developed zero-tolerance policies related to patient confidentiality.

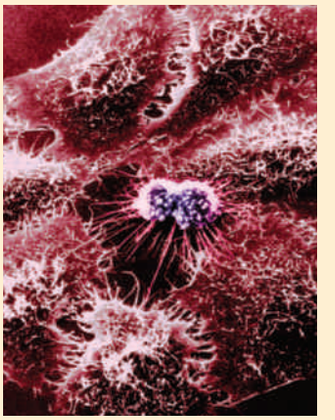
Accrediting bodies such as the Joint Commission adjust to the changing privacy and confidentiality landscape through the inclusion of general standards, such as:

- Standards to comply with laws, statutes, and regulations affecting hospital operations (Joint Commission, 2012b)
- Standards to maintain information privacy and security (Joint Commission, 2012b)
- Standards to respect patient needs for confidentiality, privacy, and security (Joint Commission, n.d.).

State regulatory agencies generally take a similar approach. In response to the UCLA incidents mentioned above, however, California enacted California Health and Safety Code Section 1280.15 in 2008. This law requires that a clinic, health care facility, home health agency, or hospice prevent unauthorized access to medical information. The statute also empowers the state agency to access fines for a data breach. The law requires the entity to report the breach to the state agency and assesses a daily penalty for the failure to do so. Note that HIPAA has a similar reporting mechanism.

Ethics in Focus: Henrietta Lacks and HeLa Cells

In addition to the notoriety of informational privacy, there is the impact of proprietary privacy. Heed the story of Henrietta Lacks, the source of HeLa cells. HeLa cells are unique in the human experience because the cells, if provided with the proper environment, not only survive for more than a few days but continue to divide. HeLa cells were used in the development of Salk vaccine (polio) as well as research into cancer, AIDs, and the effect of radiation. But what of their source, Henrietta Lacks? Lacks, an African American, was born on August 1, 1920. At age 14 she married, having already delivered two children. After the birth of her fifth child in 1951, she began bleeding abnormally. She was referred to Johns Hopkins as the nearest facility that would treat Black patients. She was diagnosed with cervical cancer, and while undergoing surgical treatment, an additional portion of the tumor was removed without Lacks's permission. Dr. George Gey was given the tissue culture and identified the HeLa cell. Lacks was admitted to Johns Hopkins in August 1951; but the cancer had metastasized throughout her body, and she died on October 4. Lacks received no compensation for her cells, which went on to further many important kinds of research. When the family began to receive requests for blood samples from researchers in the 1970s, they realized that Henrietta Lacks was the source of HeLa cells.



CDC/Phanie/SuperStock

HeLa cancer cells have proved invaluable in medical research, yet they were taken from a patient and cultured without her knowledge or approval, raising an ethical debate on the concept of proprietary privacy.

Law in Focus: Who Owns Your Cells?

Moore v. Regents of University of California (1990) explores the question of whether human tissue remains a person's property after it is removed from them, and therefore whether the removal could support an allegation of conversion, or unlawful taking of someone else's property. In this case, the plaintiff, John Moore, claimed that researchers took (converted) something that belonged to him—his blood. Under vicarious liability—and due to their authority over the researchers—the Regents of the University of California were named as defendants, though they did not do the actual taking. The case had five defendants: Dr. David W. Golde, the Regents of the University of California, a researcher, the Genetics Institute (a corporation formed by Golde), and Sandoz, the pharmaceutical company. Having been diagnosed with leukemia, on October 5, 1976, Moore went to UCLA and saw Golde. While under treatment at UCLA and on Golde's advice, Moore had a splenectomy and subsequently returned numerous times from Seattle for further testing. During each visit, samples of blood, blood serum, bone marrow aspirate, and semen were collected. Unknown to Moore and without his consent, the defendants engaged in research on the cells removed from him. The defendants concealed their actions from Moore and knew from the outset of a potential for substantial economic benefit to be derived from the cells. In 1981 the defendants filed for a patent based on Moore's cell line. Moore filed a lawsuit alleging 13 civil wrongs. The lower court thought all 13 were based on one issue, that of conversion. Therefore, the lower court evaluated only whether the defendants converted Moore's blood.

(continued)

Law in Focus: Who Owns Your Cells? *(continued)*

The lower court found no conversion, and Moore appealed to the Court of Appeals. The Court of Appeals reversed the lower court and found that the original complaint was correct. The California Supreme Court then reversed the Court of Appeals and ruled that the finding of conversion would not stand. Importantly, the California Supreme Court did preserve Moore's allegations that were based on consent; that is, that the defendants, in obtaining Moore's consent, had a duty to disclose the possible economic benefit. The court based its reasoning on a patient having a right to control his or her own body and a right to consent to medical treatment, as well as on the fact that the treating physician has a duty to disclose any material information that might affect that decision—such as the possibility that the defendants could gain substantial economic benefit. As for the conversion, this was the first time a court had examined whether conversion would apply to a patient's blood. Overall, the court faced a question of whether to create new liability—that a person continues to have a property interest in his or her bodily tissues even when those tissues are separated from the body and therefore, if the tissue is wrongfully taken or used, liability would result. To answer the question, the court weighed the potential benefit to plaintiffs like Moore versus the adverse impact on research. It seems that at the time, thousands of human cell lines were already routinely copied and distributed to researchers through tissue repositories. If the donors of the cell lines continued to own them, then every time an economically promising cell line was identified, the researcher or repository would be potentially liable to the donor. Therefore, the court did not create a new liability. However, the court did reaffirm the applicability of informed consent and the duties of practitioners in obtaining informed consent.

Discussion Questions

1. Some would argue that the question of whether body tissue remains the property of the person is not one for the courts to answer. Instead, personal autonomy is a bedrock concept of our legal system, which already respects the individual's uniqueness and right to refuse or consent to treatment. Similar to this is the concept that an individual cannot be used to benefit another without consent or compensation—for example, the prohibition on slavery. Therefore, it is inconsistent with personal autonomy to find that body tissue loses its uniqueness once separated from the individual. Do you agree or disagree, and why?
2. In weighing the effect of recognizing a cause of action for the conversion of human tissue, the court considered the effect on research. Discuss whether the court should have also considered how a marketplace in human body parts affects human dignity, and what impact the competitive bidding for such materials has on research and development.
3. If the court chose to find a cause of action for conversion, how could it have been constructed or limited to meet the majority opinion's concerns?

Shifting from a Rights-Based Approach to Compliance-Based Regulation

Like the court system, statutes, accreditation standards, and regulations seem similarly hesitant to protect patients' rights to privacy. As health information has become more accessible, legislation has been compelled to balance the right of personal privacy with the public benefit of access to such information. Existing laws, regulations, and guidelines are designed to prevent the disclosure of PHI by health care organizations or professionals by enforcing compliance, rather than to protect a patient's right to privacy. Some perceive this to be a further limitation of the right to privacy and an increased vulnerability to intrusion, whereas others perceive this to be no more than an evolution using traditional concepts to deal with technological advances. Some will feel threatened by the mere collection in one place, or codification, of the disclosures that are already commonly accepted. This evolution will be examined more closely as we review the Privacy Act of 1974, HIPAA, GINA, and ACA in the next section.

One potential intrusion into privacy involves the increased maintenance and exchange of computerized health data, making the information vulnerable to breaches in security. Furthermore, the fact that health care–related businesses such as pharmaceutical companies, health insurers, medical device suppliers, and biotechnology firms actively seek PHI has made patient rights to health care privacy even more fragile (Terry, 2008). Health care–related companies can benefit from PHI by using the data to better target their marketing and advertising, mine the data for economic advantage, and unfairly discriminate against patients, thereby reducing a company's expenditures or costs. Many of these entities want to use a patient's PHI for reasons that—while in many cases are good for the public's health, scientific knowledge, or commercial gain—fail to help the patient achieve his or her goals for treatment and may even actively thwart treatment.

In addition to the inadequate protection of a patient's right to privacy, U.S. federal and state health care standards strongly imply that if any privacy or confidentiality rights exist in health care, they belong to the health care system and not to the patient (Terry, 2008). With the exception of common law civil action, state and national standards usually fail to provide patients with private lawsuit recourse. Instead, while a patient may alert oversight agencies about a health care provider's failure to comply with the law, it is the oversight agency that gets satisfaction through civil and criminal penalties. Many would see this as a necessary policy to adopt in order to reform tort law (seeking damages or other remedies in civil law courts) in a litigious society such as ours. However, a compliance-centered approach may inadequately protect the important rights of privacy and confidentiality of patients if current penalties and the chances of being caught failed to disincentivize the bad behavior. The severity of penalties may indeed be the question to ponder as we examine these laws. For example, will penalties that range from reputational and financial exposure to loss of accreditation (which usually means the death of the enterprise) be sufficient to limit and deter breaches of privacy?

Laws and Regulations Affecting Privacy and Confidentiality

To develop a sense of the status of privacy and confidentiality, we will look at four greatly influential and complex regulations that are helping to mold the contours of the privacy and confidentiality landscape.

Health Insurance Portability and Accountability Act (HIPAA)

Directly related to privacy and tangentially related to health care, the federal Privacy Act of 1974 highlights privacy from the government/citizen standpoint. The Privacy Act provides: "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be [list of exceptions]" (Privacy Act of 1974).

The act requires both administrative and physical security safeguards. Among the exceptions are the law enforcement purposes, congressional investigations, and the Department of Homeland Security. Certain states have equivalent statutes.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) has far-reaching implications for many different areas of health care, including insurance coverage, health care fraud and abuse, and medical liability reform. However, HIPAA is perhaps best known for its regulation of privacy and confidentiality in health care contexts. The portion of HIPAA that affects health information privacy is known as the Administrative Simplification Subtitle. The regulations based on the subtitle are divided into the Privacy Rule (45 C.F.R. Part 160 and Subparts A and E of Part 164), which restricts disclosures and limits the use of PHI without the patient's permission, and the Security Rule (45 C.F.R. Part 160 and Subparts A and C of Part 164), which establishes administrative, physical, and technical safeguards to prevent the inadvertent disclosure of electronic PHI. If a qualified statistician determines that the risk of identifying the patient from the information in question is small, or if all of the 18 specific identifiers are removed from the data, then the information is considered "de-identified" and does not fall under the definition of PHI (45 C.F.R. 164.514). The 18 identifiers are:

1. Names
2. All geographical subdivisions smaller than a state, including street address, city, county, precinct, zip code, etc.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and all ages over 89
4. Phone numbers
5. Fax numbers
6. E-mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web addresses or universal resource locators (URLs)
15. Internet protocol (IP) address numbers
16. Biometric identifiers, including fingerprints and voiceprints
17. Full face images and any comparable images
18. Any other unique identifying number, characteristic, or code (with some narrow exceptions)

As good practice and unless the contents of a patient's health record have been de-identified, the patient's health record should be broadly construed to fall under the Privacy Rule's disclosure standards.

The statute establishes a duty for health care providers to notify patients of their rights to confidentiality (including the right to receive an accounting of the disclosures made under the provisions of the act) and rights to access and, in some cases, amend their PHI (45 C.F.R. 164.526). HIPAA provides civil and criminal penalties for violations by those to whom the law applies. HIPAA initially applied only to **covered entities**, which include health care providers, health plans, and health clearinghouses. However, the Health Information Technology for Economic and Clinical Health Act of 2009 extended HIPAA's requirements to **business associates**—that is, entities likely to come into contact with or have the opportunity to access PHI that perform a business function for the covered entity (45 C.F.R §§ 160.103).

When a covered entity or business associate contemplates disclosing PHI, it must obtain written authorization from the patient prior to disclosure (45 C.F.R. 164.502(a)(1)(iv)), and must also keep close records of disclosures of PHI (45 C.F.R. 164.528). However, HIPAA provides for certain legitimate disclosures of PHI that do not require written authorization from patients (45 C.F.R. 164.512). These exemptions include the disclosure of PHI in order to facilitate medical treatment of the patient or billing, as well as other health care operations as outlined in the regulations (45 C.F.R. 164.506). HIPAA obligates covered entities to actively minimize the potential for unintended harm by imposing a duty to make a reasonable effort to disclose only the minimum necessary PHI required to achieve a legitimate and specifically exempted purpose (45 C.F.R. 164.502(b)). Covered entities also have a responsibility to appoint a privacy official as well as a contact person to field patient or health consumer complaints and train staff and employees to comply with the Privacy Rule (45 C.F.R. 164.530(a),(b)).

Regarding response to breaches and penalties: Although individuals and organizations aspire to comply with HIPAA and thereby respect a patient's privacy, the history of human endeavor is less than perfect. For unauthorized disclosures of PHI, HIPAA prescribes not only a system of penalties but also a series of notice requirements. As for penalties, see the following chart:

Violation	Minimum penalty	Maximum penalty
Individual did not know he or she had violated HIPAA	$100/violation; annual max of $25,000/repeat violations	$50,000/violation; annual max of $1.5 million
Reasonable cause and not willful neglect	$1,000/violation; annual max of $100,000/repeat violations	$50,000/violation; annual max of $1.5 million
Willful neglect but corrected within time	$10,000/violation; annual max of $250,000/repeat violations	$50,000/violation; annual max of $1.5 million
Willful neglect and is not corrected	$50,000/violation; annual max of $1.5 million	$50,000/violation; annual max of $1.5 million

The above penalties are considered civil penalties. The intentional disclosure to sell, transfer, or use PHI for personal financial gain has a fine of up to $250,000 and imprisonment for up to 10 years.

The unauthorized disclosure of unencrypted PHI creates additional notification duties to:

- Notify affected individuals within 60 days of becoming aware of the breach
- Notify major media outlets and HHS if a breach involves 500 or more plan participants
- Provide in the notice to individuals, at a minimum, five specific categories of information
- Deliver the notice by first-class mail to each affected individual's last known address

The Ponemon Institute performed a 2010 Cost of Data Breach study of U.S. companies. The study indicates that the average cost of a data breach is $214 per compromised record and $7.2 million per organization.

While the intentions behind the creation of HIPAA are to protect a patient's right to privacy and uphold confidentiality, the rules are so specific, complex, and laden with exceptions that the act is often misunderstood and inappropriately executed. Table 5.1 shows the top 10 HIPAA myths.

Table 5.1: Top 10 HIPAA myths

	Myth	Explanation
10	Patient information is still covered by HIPAA once it has been de-identified.	The HIPAA privacy rule only applies to protected health information, which by definition is identifiable. Once data has been de-identified, it is no longer covered by the rule. The rule prohibits re-identifying the data, but this may be impossible to police.
9	Patients and their family members can be held liable for violating another patient's privacy and confidentiality rights.	No. HIPAA's privacy rule restrictions do not apply to patients or their family members.
8	Employers have access to an employee's health records and personal health information.	Health care providers are prohibited from disclosing personal health information to employers without the patient's explicit written authorization.
7	Health care providers must disclose personal health information to the HIPAA-allowed entities for care-related purposes.	HIPAA allows health care providers to disclose personal health information to certain third parties for care-related purposes, but they are not forced to do so. Organizations are allowed to have stricter policy protections than HIPAA requires.
6	HIPAA disallows sharing of personal health information with a patient, family member, or other caregiver authorized by the patient.	HIPAA allows disclosure of personal health information to others that the patient explicitly authorizes.

Table 5.1: Top 10 HIPAA myths *(continued)*

	Myth	Explanation
5	Patients are entitled to a free copy of their health records.	While patients have a right to a copy of their health records, they aren't guaranteed a free copy. The provider has 30 days to furnish a copy of the records and may require patients to pay a fee for the copies. If the patient wants an electronic copy, HIPAA states that providers should accommodate such a request if possible.
4	HIPAA requires patients to sign an Acknowledgement of Privacy Practices form before being treated.	Health care providers have to make a "good faith effort" to secure a patient's signature on an acknowledgement form, but it is not required and a refusal to sign is not a reason to refuse to treat a patient.
3	Patients can sue health care providers for not complying with HIPAA.	HIPAA does not confer a right to sue on harmed patients. An aggrieved patient or patient's family may complain to the Office for Civil Rights of the Department of Health and Human Services. The Office for Civil Rights will determine whether to investigate a claim further and whether to assess fines.
2	Patients must not be identified in clinical situations where other patients are present.	Health care organizations are required by HIPAA to take appropriate measures to protect patient privacy and confidentiality, but that does not mean patient names cannot be called out in a waiting room.
1	It's "HIPPA."	This misspelling is sometimes committed by health law experts. Also, "privacy" is not part of the law's name – Health Insurance Portability and Accessibility Act.

The Genetic Information Nondiscrimination Act of 2008

The Genetic Information Nondiscrimination Act of 2008 (Pub. L. 110-233), more commonly referred to as **GINA**, is a U.S. congressional act that prohibits the use of a person's genetic information for purposes of health insurance and employment. The law prohibits health plans and insurers from denying coverage to healthy patrons or adjusting premium rates when based solely on a genetic predisposition, regardless of how the insurer or health plan became aware of this PHI. GINA also prohibits employers from discriminating on the basis of a person's genetic code. Though relatively obscure today (especially in comparison with HIPAA and ACA privacy provision), GINA was touted by the late Senator Edward Kennedy as "the first major new civil rights bill of the new century" (as cited in Kaye, 2013, p. 51) when the bill was passed unanimously by the Senate and with an overwhelming majority in the House of Representatives in 2008.

The law was designed with two major goals (§101):

1. Protect the public from potential discrimination
2. Allay public fears about potential discrimination in order to promote the use of genetic testing, research, and therapy.

Associated Press/Charles Dharapak

The Genetic Information Nondiscrimination Act, which was signed by President George W. Bush in 2008, prohibits employers or health care providers from discriminating against individuals based on their DNA.

Like most other federal regulations concerned with health care privacy and confidentiality, GINA opts for a compliance-centered approach by focusing on the obligations that health care organizations, providers, insurers, and employers have to comply with the law, instead of explicitly protecting the various privacy and confidentiality rights the public may possess with regard to genetic information. Unlike HIPAA, GINA does protect the public's right to sue in a court of law for discrimination—though this is only after a person has exhausted all available administrative remedies. In fact, because the law is concerned with instances of discrimination toward individuals based on characteristics not under their control, GINA shares similarities with portions of the Civil Rights Act of 1964, which protects other immutable characteristics such as race, sex, and national origin. One similarity is that just as race cannot be a basis in making hiring or promotion decisions, neither can genetic information. In addition, GINA built on the protections of HIPAA by adding genetic information to the definition of health information.

The genetic information covered under GINA includes (§103):

1. Information about an individual's genetic test results
2. Information about the genetic test results of an individual's family members
3. Information about the patient's family history of genetic disease and disorder

Genetic test refers to "the analysis of human DNA/RNA/chromosomes that detect genotypes, mutations or chromosomal changes (§103)."

The Affordable Care Act and Patient Privacy

Recall that decisional privacy protects the patient from interference with personal decisions. The implementation of the ACA has raised the question of the proper role for government in implementing the health care decisions of its citizens. Even the requirement to purchase health

insurance that contains certain mandated services can impact a patient's treatment decision. That is, whether a benefit is covered (i.e., a mandated benefit) or not can determine whether the insured will access the services or not. The ACA also provides for an **Independent Payment Advisory Board (IPAB)**. The IPAB has the task of achieving savings in Medicare without affecting coverage or quality. Although prohibited from rationing care, concerns exist that the board will directly or indirectly limit the access to care. Finally, a concern related to decisional and informational privacy is how the disclosure of patient information to the Accountable Care Organization (ACO) will impact a patient's decisions regarding whether to consent to certain health care, such as mental health care or fertility-related health care. As permitted by the ACA, the patient's utilization information will be provided to the ACO and conceivably to participating providers.

Case Study: Needle Exchange Program at a Drug Rehabilitation Clinic

You have been asked to sit on an ethics review board. The CEO of your clinic is especially interested in opening the door for a new public health research project to begin in your clinic, and you get the impression that he placed you on this review board to facilitate the project's acceptance. He wants you to report to him on how the ethics committee deliberates about this project and also requests that you give him the names of any committee members who oppose the study.

The project is sponsored by the National Institutes of Health and is designed to determine whether over-the-counter sale of sterile syringes is more effective than needle exchange programs for drug users. The study randomly assigns 500 intravenous drug users and 500 former intravenous drug users to one of two groups: The first group of participants is enrolled in a needle exchange program; the second group is given a description of the syringe packs that participants can purchase at a large discount by using a neighborhood pharmacy that your clinic's CEO co-owns.

Researchers also proposed to determine which method of needle distribution was more effective in preventing infectious diseases such as hepatitis and HIV, which are transmitted by shared needles. Subjects will be tested for these and other diseases before and after the study period. The relative statistics will then be compared to see which method was more effective at reducing infection rates. Researchers are also interested in seeing if the availability of clean needles will cause a relapse in recovered users, and so the subjects will also be tested for the presence of drugs before and after the study.

Additional potentially ethically relevant facts:

- Jane is a supervisor for the maintenance department at your clinic and, as a heroin addict in recovery, would like to take part in the study but is concerned with confidentiality since no one at the clinic knows of her prior drug abuse.

(continued)

Case Study: Needle Exchange Program at a Drug Rehabilitation Clinic *(continued)*

- Torrance is a pharmacist in your CEO's pharmacy who despises drug abuse and, if truth be told, drug abusers too.
- The research protocol calls for the subject records to be kept through the same electronic medical record system (Logistical Electronic Administrative Knowledge System, or LEAKS) that houses regular patient records (including billing), though they are in a separate database. The clinic also uses LEAKS to keep employment records.

Activity

Write a short essay outlining what you think should be done in this case, and why. Should the review committee approve the protocol? What, if any, changes should be made to the study? Identify any ethical problems that exist and attempt to identify those that may arise, then argue for a resolution or suggest ways to avoid them. Feel free to be creative with your answer but do not fabricate or assume additional facts that solve the ethical dilemma for you or allow you to circumvent the ethical dilemmas. (For example, some might argue that it is never right to operate drug exchange programs due to a perceived complicity with illicit drug use. That is a fine position to take, but for purposes of this activity, taking that approach *avoids* the question being asked, instead of resolving it.)

As you write your answer, please identify which philosophical perspective(s) is/are reflected in your answer (e.g., utilitarian, virtue ethics, etc., or any combination of these). Also identify the ethical norms and principles that helped you make your decision.

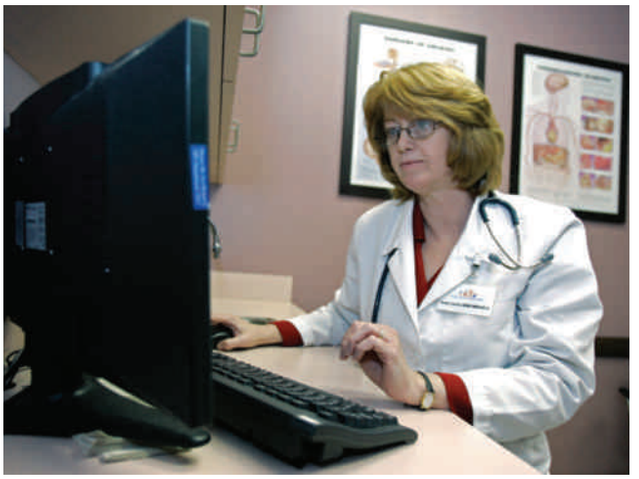
5.3 The Future of Privacy and Confidentiality

The laws discussed in the previous chapter came about primarily because technology permitted society to make certain advances not only regarding the protection of information but also to recognize benefits in sharing information. The risks and benefits of the future of privacy and technology will be characterized by the continual monitoring of technological applications to determine that the benefits merit the risks. In addition to the challenge of technology, questions currently exist regarding the basis on which individuals will trust each other at an organizational, state, and national level to share PHI and who or what is the governance of the organizations that will decide. A basic, significant question affecting informational privacy is whether the patient should even have an option to opt out of such sharing.

Confidentiality Mediated by Technology

While the importance of confidentiality has not diminished over the years, the burgeoning complexity of health care and its reliance on information technology to drive innovation and commerce has complicated the ways in which we can observe confidentiality (Terry, 2008). Americans tend to value innovation and technological progress in every corner of society, and health care is a prime example. In an increasingly fragmented health care delivery system, continuity of care and doctor–patient bonds are being replaced by a technologically mediated

care framework. In this new system, the many different, fragmented arms of health care access a core repository of health-related information. Meanwhile, the patient may or may not be directly involved in this process. The current thinking, however, is that gains in health care and costs are achievable only with the patient's participation. The concept of the patient-centered medical home is inclusive of the majority of practitioners and interventions focused on the patient, coordinated through the primary care physician using midlevel practitioners with the assistance of the electronic health record. Although quality and therefore the value of health care remains to be finally defined, it is clear that value will be the benchmark of future payment.



Associated Press/John Raoux

While electronic medical records and other technological advancements have begun to streamline the health care industry, there are growing concerns over the privacy and security of patients' digitized information.

Although there is no doubt that electronic health records and the digitization of much of our personal, medical information is an important beneficial technological advance that promises to improve the quality of care and reduce costs and medical errors, these technologies also increase the potential for risks to patients that is seldom accounted for in their utilitarian justifications (Terry, 2008). And yet, electronic health records as well as new information technologies such as cloud computing, online consultations, and Internet prescribing achieve their highest potential benefit when they are accessible throughout the medical system, flow unrestrained, and contain accurate and complete information. In the first year of reported results for Pioneer ACOs, the ACOs generated lower readmissions rates and better blood pressure control when compared to other Medicare providers. In addition, one third generated a cost savings (Centers for Medicare and Medicaid Services, 2013). Although it is rational to believe that there are benefits in care coordination, the large-scale and ongoing benefits remain to be seen. However, the concomitant risks posed by these technologies are also at their highest and most dangerous under the same conditions that render the technologies the most useful.

One of the potential avenues for abuse or breach of the duty of confidentiality is that while most private patient information is rapidly becoming computerized and more easily dispersed, the number of people who have ready access to the information is increasing at a staggering rate. Staff and employees throughout the health care system, including those at hospitals and doctors' offices, insurance companies, laboratories, allied health care entities, accounting and billing firms, and others have access to electronic health records and the private information they contain. Although laws, policies, and regulations theoretically limit the scope of disclosure, a patient's confidentiality remains easily and regularly violable. Permission is not always sought for this disclosure, nor is the patient made aware of the potential breadth of the disclosure by health care staff.

Significantly, social media affects privacy. With the advent of medical condition websites, collectives have developed for cancer and Parkinsonism patients to share information and experiences. Other websites such as CaringBridge invite patients, family, and friends to communicate regarding medical conditions. Even crowd-funding sites have developed to help patients pay medical bills. As some physicians have opted to practice concierge medicine (i.e., limiting their patient base), one of the additional benefits has been e-mail exchange with the physician.

5.4 Chapter Highlights

- In Chapter 5 we examined the often misused terms *privacy* and *confidentiality*. Privacy is an individual's expectation to keep or control access to his or her individual space as well as knowledge of certain information. Confidentiality is the ethical and legal obligation to refrain from sharing information about other people without their authorization. From their roots in the ethical norm of respecting individuals and their autonomy, we also explored these two concepts as a manifestation of a caring and trusting relationship between health care provider and health care consumer. We also investigated how these two terms have evolved as legal doctrines in the United States and surveyed a few cases that illustrate this evolution.
- From this historical overview, we examined how the ethical and legal concept of a right to privacy and commonsense expectations for confidentiality between doctors and patients has slowly been replaced by an expanding and convoluted web of policies, guidelines, accreditation standards, laws, and regulations. With the exception of common law civil action, these laws and regulations tend to focus on the rights of the health care provider, oversight agencies, and the government, rather than on those of the patient.
- We also looked at several statutes that contain privacy rules, including the ACA, HIPAA, and GINA. We examined not only their provisions, but some of the major misunderstandings and myths about these statutes. Case studies were also used to illustrate some of the essential moral bases for privacy and confidentiality, as well as the legal and regulatory contexts in which health care organizations practice.

Case Study: Genetech and Shelbyville—Community-Based Participatory Research and Privacy

The following case study affords students an opportunity not only to understand GINA as applied but also to consider the personal decisions a patient must make in choosing to be tested.

The Context

Located in the mountains in Arkansas, Shelbyville is a small, close-knit mining town that is almost entirely dependent on a large lead-zinc mining operation, SKB. This company employs much of the town and is responsible, through community outreach, for much of the town's infrastructure, education, and health service. Although Shelbyville does not have a full-service hospital, it does have a modern, well-staffed multiuse clinic that specializes in preventive and acute care. The clinic is owned and operated by SKB as part of its employee health program but is also open to nonemployee community members as well as those who cannot afford to pay for health care. You are the newly appointed general director of the clinic. You oversee all of the day-to-day health care administration duties, along with a small executive staff.

(continued)

Case Study: Genetech and Shelbyville—Community-Based Participatory Research and Privacy *(continued)*

Shelbyville, though in a beautiful location, is rather isolated from the rest of the world, and for as long as anyone can remember, there has been intermarrying among the town's six large family clans. It is a hardworking community that has recently fallen on hard times because SKB is restructuring after being bought out by a large, multinational conglomerate known as Global Synergy. There has even been talk of Global Synergy closing some of its mining operations altogether.

For more than 50 years, the townspeople of Shelbyville have been quietly aware of a terrible disease among their population. It seems that the relative homogeneity of the gene pool in the town has been partly responsible for troubling familial clusters of both hypothyroidism and Huntington's disease (HD). This disease is a genetic disorder that appears without warning between the ages of 30 and 60. It causes irreversible mental and motor deterioration and invariably leads to death after several years of intense pain and suffering for both patient and family. There is currently no known treatment or cure for this Mendelian dominant disorder (everyone who has inherited the gene will develop the disease and also transmit it to approximately half of his or her children). Preimplantation genetic diagnosis, prenatal predictive testing, and predictive genetic testing for the disease for children, adolescents, and adults only recently became available. Though the town clinic does not have the capacity to do genetic testing, it has been treating the sufferers and sending care nurses and physicians to the sufferers' homes for chronic treatment, which is very expensive. Local and state laws do not require that a diagnosis of HD be reported to public health authorities.

As the general director of Shelbyville's health clinic, you are concerned about the high incidence of HD in your community. In an effort to help your medical staff learn how to better diagnose, assist, and counsel those affected by the disease, you recently sent one of your clinic's young physicians to an HD medical conference in St. Louis, Missouri.

While there, the physician spoke with an HD genetic researcher who described the importance of acquiring a large genetic database with a high incidence of HD in order to help his pharmaceutical company–sponsored researcher to better understand, and hopefully find a cure for, this horrible disease. The researcher also mentioned that he would be willing to pay a one-time, $150,000 finder's fee to anyone who would locate a source site for this kind of database. The physician told the researcher that he had just this kind of cluster back home. The researcher makes immediate plans for his research to focus on Shelbyville.

The Problem

The St. Louis researcher arrives in Shelbyville with a genetic database research protocol approved by a central IRB and makes plans to call for volunteers from among the clinic's patients, advertise heavily in the local media, and deploy a small army of recruiters and study personnel in your community. On the same day that the researcher arrives, you receive several faxes from the Community-Based Participatory Research and Development arm of Genetech. A quick Internet search shows that Genetech is the pharmaceutical sponsor of the trial as well as a wholly owned subsidiary of Global Synergy (the global conglomerate that owns SKB, and by extension, your clinic). While at first you were excited about the potential of an HD research study based in Shelbyville, you soon realize that there might be much reticence among the population to participate in a trial that may risk publicly portraying the town in a negative light. You are also concerned about the fact that the clinic, the mine, and the biotech firm conducting the research are all owned by the same entity.

(continued)

Case Study: Genetech and Shelbyville—Community-Based Participatory Research and Privacy *(continued)*

To allay any fears you may have, Genetech agrees to include other disorders in the protocol. This way, HD will not call as much attention to itself. Additionally, the information will be de-identified and securely locked in a file cabinet at the clinic as well as on several researcher laptops and a Genetech computer server operated by Global Synergy. These precautions are in place to protect the subjects' privacy and to ensure that no one but the subjects, if they request it, will be made aware of the status of HD for themselves and the probability of transmitting it to their offspring. Due to this internal agreement at Genetech, the protocol's lengthy, jargon-filled informed consent form says that the study is aimed at compiling a genetic information database in order to look at the problem of the prevalence of hypothyroidism in the small community. Part of the consent form reads: "By signing this document, I also consent to having my de-identified sample used for other research to help find cures for other genetic diseases such as, but not limited to, Tay-Sachs disease, sickle-cell anemia, and Huntington's disease." This is the only mention made of HD in the informed consent document. The document also states that there is little chance of the subject obtaining any personal or direct benefit from the research. As part of the IRB review, Genetech was obliged to obtain community consent for the research and has scheduled a town hall meeting to discuss the research and obtain the consent of the community before proceeding. Before the town hall meeting is scheduled to occur, the city council of Shelbyville has formally requested that you write a short recommendation for what the city of Shelbyville should do.

Activity

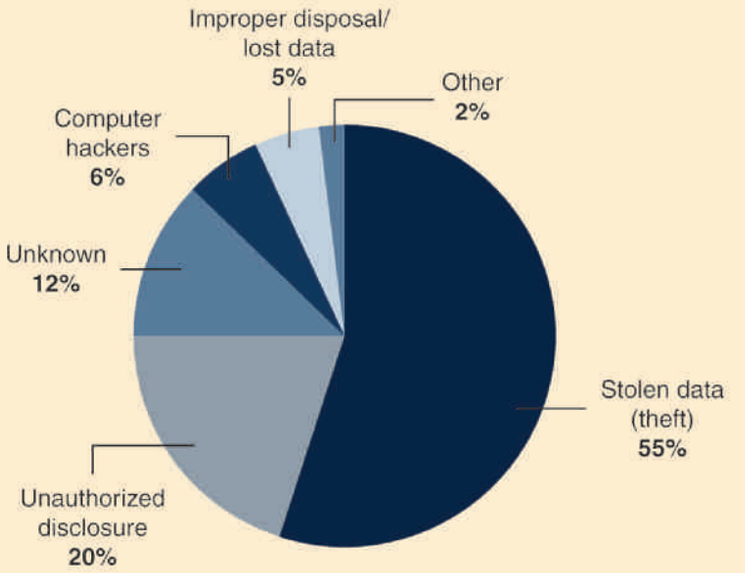
Write a short (one page or less) recommendation that you will present at the Shelbyville town hall meeting in a few days. In this recommendation, address all of the following:

- Explain briefly and in understandable language what the proposed research is for and what benefits, if any, might be expected.
- Describe the risk potentials for enrolling in the study, to the best of your current knowledge.
- Identify and explain all of the ethical and legal issues surrounding the proposed research study.
- Explain any potential risks to the insurability of the townspeople.
- Make a recommendation to the townspeople about providing the requested consent for this research to take place in Shelbyville and state whether you think that participation is a good idea for the community.
- Present any suggestions for negotiating with Genetech or requesting any assurances.

Case Study: Ongoing HIPAA Violations

Frequency of Certain HIPAA Violations, 2010–2013

Between March 3, 2010, and August 26, 2013, the U.S. Department of Health and Human Services documented 659 cases of HIPAA violations that affected 500 or more people per incident.



Source: U.S. Department of Health and Human Services. (2013). Breaches affecting 500 or more individuals. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

The U.S. Department of Health and Human Services' Office for Civil Rights (OCR) is responsible for HIPAA enforcement. The OCR posts the top five issues in investigated cases (see Top Five Issues in Investigated Cases Closed with Corrective Action, by Calendar Year).

Top Five Issues in Investigated Cases Closed with Corrective Action, by Calendar Year

Year	Issue 1	Issue 2	Issue 3	Issue 4	Issue 5	# of Complaints
2010	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Notice	8,764
2009	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Complaints to Covered Entity	7,587
2008	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Complaints to Covered Entity	8,730
2007	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Notice	8,221

Source: U.S. Department of Health and Human Services, Office for Civil Rights, n.d.b.

(continued)

Case Study: Ongoing HIPAA Violations *(continued)*

You will notice that the top five issues in the list are remarkably constant from year to year.

Below are examples provided by the OCR that illustrate the enforcement issue of Impermissible Uses and Disclosures as listed in the "Issue 1" column in the Top Five Issues in Investigated Cases Closed with Corrective Action chart:

> Pharmacy chain: "A chain pharmacy disclosed protected health information to municipal law enforcement officials in a manner that did not conform to the provisions of the Privacy Rule. Among other corrective actions to resolve the specific issues in the case, OCR required this chain to revise its national policy regarding law enforcement's access to patient protected health information to comply with the Privacy Rule requirements, including that disclosures of protected health information to law enforcement only be made in response to written requests from law enforcement officials, unless state law requires otherwise" (U.S. Department of Health and Human Services, Office for Civil Rights, n.d.a).
>
> Hospital messages: "A hospital employee did not observe minimum necessary requirements when she left a telephone message with the daughter of a patient that detailed both her medical condition and treatment plan. An OCR investigation also indicated that the confidential communications requirements were not followed, as the employee left the message at the patient's home telephone number, despite the patient's instructions to contact her through her work number" (U.S. Department of Health and Human Services, Office for Civil Rights, n.d.a).
>
> Health plan: "An employee of a major health insurer impermissibly disclosed the protected health information of one of its members without following the insurer's authorization and verification procedures" (U.S. Department of Health and Human Services, Office for Civil Rights, n.d.a).
>
> Health system: "A nurse practitioner who has privileges at a multi-hospital health care system and who is part of the system's organized health care arrangement impermissibly accessed the medical records of her ex-husband" (U.S. Department of Health and Human Services, Office for Civil Rights, n.d.a).

Breaches reported by the California Department of Public Health (2013) include:

> Employee text: An admitting clerk in the hospital's Occupational Health Department accessed and used the health information of a patient. The patient informed the facility that he received a sexual text message from employee A. Employee A admitted that he sent the message and that he had sent messages to approximately eight to ten other patients over a 1-year period.
>
> Employee to employee: Patient A, a hospital employee, was admitted to the hospital. The risk manager performed an audit regarding who accessed patient A's medical record as a matter of routine. Patient A told coworker C that he was in the hospital. Coworker C told coworker B, and coworker B accessed patient A's medical record. Coworker B told patient A of the access and apologized.
>
> RN flash drive: In preparation for attending a conference, an RN, contrary to policy, downloaded the patient information of 209 patients on an unencrypted flash drive. The RN intended to work on a quality project while away. When the RN returned, he realized that he had lost the flash drive. The RN stated that he forgot there was a policy regarding the use of flash drives.

(continued)

Case Study: Ongoing HIPAA Violations *(continued)*

Discussion Questions

In the above cases, some employees were terminated and a number of organizations fined. Yet these problems continue to occur.

1. Consider the above examples and discuss if there are common issues. In particular, does the law regarding privacy exceed the limits of human self-restraint?
2. The elements of compliance are compliance standards; high-level administrative oversight; employee screening; education; monitoring systems; employee discipline; responses to violations; and periodic reassessment. If you were the compliance officer of these organizations, what would your compliance plan contain to reduce or eliminate the above breaches?

Critical Thinking and Discussion Questions

1. For the following circumstances, write down whether you feel that the person with access to protected health information (PHI) should have access to that information, and why. Ask yourself if the access is necessary to achieve a necessary and legitimate purpose and whether that necessity is sufficient to override the weighty rights of privacy and confidentiality that individuals are generally granted in the United States.
    a. In a situation in which an unconscious patient is in need of immediate help, an emergency department doctor wants to know what medications, treatments, and research studies the patient has taken or been a part of recently in order to better diagnose and treat the patient.
    b. A patient is referred to a podiatrist for treatment of pain associated with fallen arches. The podiatrist not only has access to a patient's orthopedic medical history and medications, but also records of treatment for sexual dysfunction and mental health issues.
    c. A unit director in a large medical center finds out that one of her team members is pregnant, and she would like to give her a baby shower. However, she does not know when the baby is due or the sex of the baby but could find out the answer to both of these questions very easily by accessing her team member's electronic health record.
    d. The CFO of a hospital tries to recover some of the unpaid debt owed by patients by hiring a debt collection agency. The CFO arranges for a debt collection agent to borrow some scrubs from the hospital, hang out in the emergency department, and check every registered patient's records to see if any currently owe the hospital money. Whenever he finds a patient in arrears, he approaches the patient to pressure him or her into payment.
2. How might one reduce or eliminate the temptation that health insurers and employers may have to contain their costs by accessing confidential patient information?
3. Name three advantages and three pitfalls to electronic health records.

4. What steps could a chief information officer take to minimize the chances of having personal health information (PHI) disclosed inappropriately in his or her health care organization?
5. Describe one instance in which confidential information may be legally disclosed without the patient's consent under the rules of HIPAA.
6. Which of the following is a federal law that prohibits insurers and employers from discriminating against someone based on their genetic information?
    a. ACA
    b. HIPAA
    c. GINA
    d. EMTALA
7. Describe the difference between privacy and confidentiality in health care settings.
8. Why might certain health care–related businesses covet protected health information (PHI) when they have no medically related interest in the care of the patient?
9. Describe one argument for why a compliance-centered approach would be worse at protecting patient privacy and confidentiality than a rights-based approach.
10. Describe one argument for why a rights-based approach would be worse at protecting patient privacy and confidentiality than a compliance-centered approach.

Key Terms

business associate Under HIPAA, an entity that performs a business function for the covered entity and is likely to come into contact with or have the opportunity to access protected health information.

confidentiality The ethical and legal obligation not to disclose the information of those who have entrusted it to someone else. Respecting a person's rights to privacy and confidentiality is a general obligation that we all have toward all others, but the duty is especially weighty in health care relationships based on trust.

covered entity Under HIPAA, a health plan, health clearinghouse, or health care provider that transmits electronic health information.

decisional privacy The aspect of privacy that concerns limiting interference with a person's decisions.

Genetic Information Nondiscrimination Act of 2008 (GINA) U.S. congressional act that prohibits the use of a person's genetic information for purposes of health insurance and employment.

Health Insurance Portability and Accountability Act (HIPAA) The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of health information needed for patient care and other important purposes.

Independent Payment Advisory Board (IPAB) Under the Affordable Care Act, an appointed group of experts, to be confirmed by the Senate, who recommend policies to control Medicare costs. IPAB recommendations will become law unless they are specifically rejected by Congress within a strict time framework.

informational privacy The aspect of privacy that concerns the access to personal information.

physical privacy The aspect of privacy that concerns limiting access to a person and intimate spaces.

privacy An individual's expectation to keep or control access to his or her individual space as well as knowledge of certain information. What legally falls under this "zone of privacy" often varies, depending on the jurisdiction or the context, and the expectations of privacy can also vary by person, context, or culture.

proprietary privacy The aspect of privacy that concerns retaining ownership interests in the person's body.

protected health information (PHI) Protected health information encompasses a large array of patient and treatment details, especially those that have the potential to identify a patient. It is commonly considered a safe assumption that any part of a patient's health record (including payment history) is likely to be considered protected health information.

right to privacy The general right to be left alone. It is the means by which access to intimate details and information is controlled by the person. In legal terms the right to privacy also encompasses the right to limit the interference of others when making personal and autonomous choices.