Chapter 13
Medical Records and Confidentiality: Evolving Liability Issues Inherent in the Electronic Health Record, HIPAA, and Cybersecurity

James E. Szalados

The Legal Basis of Privacy Protections

Privacy is defined simply as "freedom from unauthorized intrusion" [1] – in general, a person's right to be free from unwanted publicity and scrutiny without their consent. The right to privacy is also defined as the "right of a person to be free from intrusion into or publicity concerning matters of a personal nature" [2]. Privacy enables individuals to create boundaries and insulate themselves from unwarranted interference. The notion of a right to control one's self is universally understood, and generally recognized, because that right is rooted in principles of personal property, liberty, autonomy, and personhood. Privacy, then, is widely held to be a fundamental human right and is the foundation for the respect for human dignity.

Although the right to privacy is a fundamental human right recognized in the United Nations Declaration of Human Rights, by the constitutions of most countries, and by the majority of world courts, it is not universally conferred. Historically, Plato argued that the complete life of the individual was to be determined by the state and its aims, and consequently there was no place for individual freedom and autonomy. Furthermore, the natural philosophers, including Mill and Locke, did not see privacy right as a societal value; rather, they viewed the individual as a member of the larger community. The right to one's privacy is similar to other fundamental human rights and can be subjugated to competing interests or authoritarianism and

J. E. Szalados (✉)
Director, Surgical and Neurocritical Care Units, Rochester Regional Health System at Rochester General Hospital, Rochester, NY, USA

The Szalados Law Firm, Hilton, NY, USA
e-mail: james.szalados@rochesterregional.org; jszalados@aol.com

J. E. Szalados (ed.), *The Medical-Legal Aspects of Acute Care Medicine*,
https://doi.org/10.1007/978-3-030-68570-6_13

can easily also be either involuntarily or voluntarily surrendered. Indeed, through technology, individuals are surrendering privacy rights in an unprecedented manner.

The American legal definition of privacy is rooted in American culture, although privacy is not an express individual right in the US Constitution. In fact, the US Supreme Court first recognized a right to privacy in the case of *Griswold v. Connecticut*, where, the Court, in its ruling in a case challenging a statute which had criminalized contraception, derived, or extrapolated, a right to privacy through penumbras otherwise inferred from explicitly stated constitutional protections. The *Griswold* court held that an implied right to marital privacy could be reasonably inferred from individual rights explicit within the First, Third, Fourth, Fifth, and Ninth Amendments, so that when the inherent penumbras are taken together, the Constitution can reasonably create a "zone of privacy." [3]

Thus, aspects of The Bill of Rights may reasonably be construed to suggest a right to aspects of privacy, for example:

1. The First Amendment, addressing the privacy of beliefs ("Congress shall make no law respecting an establishment of religion…")
2. The Third Amendment, addressing a right to privacy within the home ("No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner…")
3. The Fourth Amendment, addressing a right to privacy of person and possessions ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…")
4. The Ninth Amendment, addressing a general right to privacy ("The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.")
5. The reiteration of the importance of personal liberty within the 14th Amendment ("No State shall... deprive any person of life, liberty, or property, without due process of law.")

Although many will find it remarkable that there is no clearly articulated right to personal privacy within the Constitution, the Constitution does articulate, perhaps more so than any other founding document in the history of civilization, deep respect for property, liberty, autonomy, and personhood. Nonetheless, despite past judicial rulings, the right to privacy in the United States remains open to debate and to future court interpretation.

Perhaps the strongest formal articulation regarding the importance of privacy is found not within the constitution but rather in early American jurisprudence. Justice Brandeis stated, somewhat presciently, within a ruling dissent in 1928 that:

> Moreover, 'in the application of a Constitution, our contemplation cannot be only of what has been, but of what may be.' The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home…

> The principles laid down in this opinion affect the very essence of constitutional liberty and security. They reach farther than the concrete form of the case there before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employees of the sanctities of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property…
>
> The protection guaranteed by the amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. Justice Brandeis's dissent in Olmstead v. U. S. [4] (1928)

Although Brandeis, in *Olmstead,* referred specifically to a right to privacy from governmental intrusion, he continued to explore the importance of personal privacy within society as a whole, within the context of "political, social and economic changes" [5]. Following the publication of "The Right to Privacy," Warren and Brandeis were largely credited with establishing the invasion of privacy tort into American jurisprudence.

Contemporary state tort laws widely recognize a cause of action for "invasion of privacy" in settings and situations where a "reasonable expectation of privacy" would apply. Invasion of privacy constitutes an intentional tort, thus requiring proof of an intent to intrude upon the affairs of another, where there would otherwise be a reasonable expectation to be left alone. Prosser classifies invasion of privacy [6] claims into four general types:

(1) Intrusion of Solitude: "consists solely of an intentional interference with his interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man" [7].
(2) Appropriation of Name or Likeness: "the interest of the individual in the exclusive use of his own identity, in so far as it is represented by his name or likeness, and in so far as the use may be of benefit to him or to others" [8].
(3) Public Disclosure of Private Facts: "one who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public" [9].
(4) False Light: the protection of one's reputation [10].

Brandeis and Warren recognized in 1890 that privacy was an important personal right and that new and evolving technology could and would alter our individual relationships with the matter we would hold private. The technologies which Brandeis and Warren saw in evolution, at the time they considered the impact of technology, were telephone, telegraph communications, and cameras. With the subsequent development of computer technology, the ability to store and transmit large volumes of information electronically supported a widespread perception that

technology could further jeopardize privacy, resulting in a slow promulgation of legal and regulatory safeguards [11].

Nonetheless, over the course of the past decade, the personal importance of individual privacy is arguably fading whereas a new perception of privacy as a norm that regulates and structures social life (the social dimension of privacy) is gaining ever-increasing importance in legislation, law, relationship, popular culture, and commerce [12]. Some would argue that in the age of social media and the Internet, despite the inherent risks, many of the things that Americans previously considered to be inviolably private are increasingly accepted as reasonably pubic [13].

A Distinction Between Privacy and Confidentiality

Privacy is an expectation based on autonomy; to a large degree it is a right, a right controlled by the holder, and therefore surrendered at will. Confidentiality on the other hand is a duty owed to another, restricting the use and dissemination of private information; the duty of confidentiality is ethical and legal. Confidentiality is a key element of the fiduciary relationship between professionals and their clients/patients. Privacy is a quasi-right rooted in common law, whereas confidentiality is an ethical and/or legal duty. Confidentiality refers to the protection of privileged information. Therefore, from a legal point of view, privacy and confidentiality have distinctly different meanings.

Reasonable expectations of privacy attach to certain places, things, and activities, for example, your home, your bedroom, your mail, your telephone calls or text messages, public bathrooms. Duties of confidentiality, on the other hand, apply to information shared, with the expectation that it be held in confidence, on the behalf of another, and shared only if and when appropriate authorization has been provided by the one to whom the duty of confidentiality is owed. Examples of confidentiality include information held on one's behalf by those legally empowered to do so; banks or federal or state agencies; health information privacy in the custody of healthcare providers; confidentiality mandated by contract such as confidentiality or nondisclosure agreements; or confidentiality dated by privilege, such as the attorney-client privilege, the patient-physician privilege, spousal privilege, and the priest-parishioner privilege. Privileged communications and information represent the highest level of civilian privacy and confidentiality; privileged communication refers to the exchange of, and the information exchanged between, two parties in which the law recognizes a private, protected relationship where the communication is protected by law.

In legally recognized protected relationships wherein the communication is expected to be in private and where a duty of privilege applies, the rights for protection for the communication belong to the client, patient, or penitent. The recipient of the information must keep the communication private, unless the privilege is waived by the discloser of the information, in other words, the holder of the

privilege. Confidentiality is a duty; privilege is a rule of evidence by which confidentiality is protected.

The attorney-client privilege is the oldest privilege recognized by western jurisprudence, with its beginnings in the Roman Republic, subsequently established in English law as early as the reign of Elizabeth I in the sixteenth century [14]. The privilege afforded to confidential communications between client and attorney was recognized at common law and is now well established in the US Federal Courts [15]. At the most basic level, the attorney-client privilege is essential to justice. The court in *United States v. Grand Jury* Investigation noted that:

> … although the law strives to ascertain the truth, there exists a countervailing policy of insuring the right of every person to freely and fully confer with and confide in a person having knowledge of the law and skilled in its practice, so that adequate advice may be received and proper defenses asserted. Such assistance can be given only when the client is free from the consequences of apprehension or disclosure by reason of the subsequent statements of his own skilled lawyer. [16]

Thus, the attorney-client privilege, firmly grounded in the confidential nature of the relationship, allows for honest and complete disclosure of the relevant facts and impressions by a client to his or her legal counsel. Since the client can rest secure in the knowledge that his or her statements cannot be construed against his or her interest, that candid and open communication will then allow the attorney to provide accurate and well-reasoned professional advice based on a complete understanding of all the facts and issues at hand. The privilege in effect creates a legally protected "zone of privacy" essential to the relationship [17]. The rules regarding attorney-client privilege will vary between jurisdictions. However, in general the scope of privilege is defined:

> (1) Where legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose,
> (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) except the protection be waived. [18]
>
> Wigmore on Evidence. 1961.

An attorney-client privilege exists when there is an attorney-client relationship; and the meaning of "relationship" is broadly construed. The attorney-client relationship presupposes a "reasonable belief" that an attorney-client relationship indeed exists. An express contract is not necessary to form an attorney-client relationship; the relationship may be implied from the conduct of the parties. The court opinion in *Togstad v. Vesely* extended the definition of the attorney-client relationship to non-clients if: (1) the non-client seeks legal advice, (2) then the non-client reasonably relies on that advice as legal advice, and (3) the attorney does not attempt to dissuade the non-client from relying on the advice [19].

Nonetheless, the simple act of communicating information to an attorney does not render the information, itself, confidential. Where the information communicated is public, known to or in the possession of another, then the underlying information itself is not privileged [20]. Communications with an attorney, even if

stipulated that they be in confidence, will not prevent the underlying facts from compelled disclosure, if that information can be found in the public domain or discovered from a non-privileged source [21].

Privilege applies only to private information that is communicated in confidence. In addition, the privilege belongs to the client, who is the "holder" of the privilege, and the client has the authority either to assert the privilege or waive it. The mere presence of a third party compromises confidentiality and can negate the creation of an attorney-client privilege; similarly the privilege may be destroyed or waived by a careless, unintentional, or inadvertent disclosure. Where the privilege is waived, intentionally or inadvertently by the client, the confidential nature of the information is destroyed; on the other hand, where the attorney, either deliberately or negligently, discloses privileged information, then he or she may be found liable for legal malpractice.

Privacy and Confidentiality Within the Healthcare Context

The privacy and confidentiality of medical records is a well-established principle of both medical ethics and health law; and the confidentiality of communications in the healthcare context is the basis for the patient-physician privilege. Once again, privacy refers to the nature of the information conveyed, confidentiality refers to the duty to hold the private information securely and in confidence, and privilege refers to the rule of evidence that protects the confidential communication from a compelled disclosure.

In the same manner that honest, thorough, and candid communications between attorney and client are essential to promote the interests of justice, during the therapeutic encounter, the private communications between patient and physician serve to promote the best medical interests of the patient. Without trust, patients will not freely reveal their personal health information, and the scope and quality of the medical encounter are subsequently jeopardized.

The importance of confidentiality to the relationship between the patient and their health care provider has been repeatedly affirmed as a professional responsibility of physicians since antiquity and is exemplified by the professional oaths of medicine. The Classical Version of the Oath of Hippocrates states:

> ...Whatever, in connection with my professional service, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret. While I continue to keep this Oath unviolated, may it be granted to me to enjoy life and the practice of the art, respected by all men, in all times. But should I trespass and violate this Oath, may the reverse be my lot. [22]

Therefore, as professionals, physicians and providers are obligated by a fiduciary duty to protect the privacy and confidentiality of their patients, their health information, and the relevant confidential communications. A "fiduciary duty" is one which a professional owes to a beneficiary by virtue of his position of trust, within the

setting of inequality of knowledge, training, and/or experience. Thus, fiduciary principles impose a heightened duty of loyalty, integrity, and devotion on physicians. A breach of the duty confidentiality also fundamentally undermines the expectation of confidentiality and the presumption of compete trust inherent in the physician-patient relationship.

> There is no real doubt, of course, that the relationship between a doctor and his patient is one in which the patient normally reposes a great deal of trust and confidence in the doctor, accepting his recommendations without question. … The relation of physician and patient has its foundation on the theory that the former is learned, skilled, and experienced in those subjects about which the latter ordinarily knows little or nothing, but which are of the most vital importance and interest to him, since upon them may depend the health, or even life, of himself or family; therefore the patient must necessarily place great reliance, faith, and confidence in the professional word, advice, and acts of the physician. [23]
>
> Witherell v. Weimer (1981)

The ethical foundations of the patient-physician confidentiality extend to well-established legal ramifications; these include, but not limited to, breaches of privacy, confidentiality, loyalty, and contract. Disclosure of confidential medical information to outsiders may have associated "damages" and can lead to severe emotional, social, or economic injury as well as humiliation, social stigma, loss of reputation, job, insurance, or marital relationship. Confidential communications during psychiatric treatment or psychotherapy are afforded a heightened level of privacy protection; even where consent is obtained for the release of medical records, psychiatric and psychological treatment information must be redacted and separated from the disclosure; and separate consent is generally required for the release of such sensitive records.

Until recently, there was no single pervasive body of US legislation which uniformly and comprehensively covered the protection of private and personal health information; instead, the confidentiality of health information was afforded some protection through a myriad of federal and state laws and case law.

The Federal Privacy Act of 1974 established standard information practices to address the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies [24]. Although the act did not apply to private sector healthcare facilities, it was nonetheless important because it was among the first legislation enacted which recognized the threat to privacy resulting from the accumulation of large amounts of personal information in computerized databanks or government files. The act is considered limited in application because it was limited by vagueness and imprecision [25]. The Joint Commission, in its 1990 standards, required that medical records be accurate, accessible, authenticated, organized, confidential, secure, current, legible, and complete [26].

The duty to maintain confidentiality has always been balanced against the duty to breach confidentiality under some circumstances. For example, mandatory reporting laws regarding transmissible diseases, injuries related to crimes, or cases of abuse, neglect, or exploitation require disclosure of relevant health information to authorities, even in the absence of patient consent. The first American public health

laws addressing surveillance regulations were enacted in Rhode Island in 1741; the law required tavern keepers to report persons with infectious diseases to local health officials [27]. Public health exceptions to privacy have historically presented a dichotomous challenge to clinical ethics and the patient-physician relationship.

The primary analysis of clinical ethics relates to the resolution of ethical and moral dilemmas between healthcare providers and their individual patients during the process of clinical care. On the other hand, the relevant analysis for public health, where the focus is population and community well-being, the community rather than the individual is the patient. The dominance of individual autonomy despite prima facie equivalence in clinical ethics is incompatible with the population-centered focus of public health [28].

The California Supreme Court, in *Tarasoff v. Regents of California*, imposed an affirmative duty on physicians to breach the confidentiality of the patient-physician relationship. The California Supreme Court heard the case twice, and the subsequent legal doctrine is based upon the outcome of two rulings: Tarasoff I (1974) and Tarasoff II (1976). In brief, the case involves a man named Prosenjit Poddar, then a student at the University of California at Berkeley, and a woman named Tatiana Tarasoff who met at a dance class in 1968. Poddar took a liking to Tarasoff; however, she did not reciprocate. Poddar developed a mental conflict stemming from the failed relationship and sought help from a counselor at Cowell Memorial Hospital to whom he disclosed that he was going to kill Tarasoff. The psychiatrist, Dr. Moore notified the campus police who interviewed Poddar and then released him. Upon learning of the circumstances, the then director of psychiatry, Dr. Powelson, demanded the destruction of all clinical notes as well as the letter which was sent to the campus police by Dr. Moore regarding Poddar. Poddar then went to the home of Tarasoff, where he shot her with a pellet gun and stabbed her numerous times, killing her. Tarasoff's parents filed suit against the University of California, resulting in the 1974 Tarasoff I decision [29] and in the "duty to warn" or "Tarasoff doctrine," which required mental health providers to warn potential victims. In its decision, the court relied on

> the Principles of Medical Ethics of the American Medical Association (1957) section 9: "A physician may not reveal the confidences entrusted to him in the course of medical attendance . unless he is required to do so by law or unless it becomes necessary in order to protect the welfare of the individual or of the community." (Emphasis added.) We conclude that the public policy favoring protection of the confidential character of patient-psychotherapist communications must yield in instances in which disclosure is essential to avert danger to others. The protective privilege ends where the public peril begins. … For the reasons stated, we conclude that plaintiffs can assert the elements essential to a cause of action for breach of a duty to warn. … The majority's opinion correctly holds that when a psychiatrist, in terminating treatment to a patient, increases the risk of his violence, the psychiatrist must warn the potential victim.
>
> Tarasoff v. Regents of California, 1974.

The court heard the case again in 1976, where, in Tarasoff II [30], the ruling was extended from a "duty to warn" potential victims but also to take reasonable precautions to protect potential victims from known dangers by patients. Nonetheless, the

Table 13.1 Civil Monetary Penalties (CMP) under HIPAA [62]

Tier	OCR penalty discretion	OCR penalty discretion	Minimum penalty per violation	Maximum penalty per violation	Annual aggregate limit for identical violations
Tier 1	No knowledge	Waive or reduce	$ 100	$ 50,000	$ 25,000
Tier 2	Reasonable cause	Waive or reduce	$ 1000	$ 50,000	$ 100,000
Tier 3	Willful neglect corrected	Penalty mandatory	$ 10,000	$ 50,000	$ 250,000
Tier 4	Willful neglect Not corrected	Penalty mandatory	$ 50,000	$ 50,000	$ 1,500,000

California *Tarasoff* ruling, notwithstanding, states different states have taken different points of view regarding the duty to warn or the duty to protect (Table 13.1). Since the *Tarasoff* rulings were in California State Court, they are at best persuasive; at present 23 states have enacted statutes mandating reporting; 11 states maintain a permissive posture; and others have established neither precedent nor statute to guide clinicians. The laws change, and it is incumbent on providers to be familiar with the exact nature of the laws of the state in which they practice. Furthermore, a recent review of court decisions involving Tarasoff issues, even states with existing statutes did not uniformly rely on them in their decisions underscoring the importance of clinical and ethical judgment [31] and perhaps institutional protocols.

The Medical Record

The medical record is a repository of a vast amount of a patient's personal information; it includes information on lifestyle choices, social history, past and current medications, past and present medical, surgical and psychiatric diagnoses, treatments, physical examination findings, responses, laboratory and radiologic data, and photographs. In addition, the medical record also includes assessments of medical necessity and the subjective impressions and opinions of providers, making the medical record, in a sense, a "work product." A variety of providers and clinicians enter documentation into the medical record, for example, therapists, nurses, and social workers. Since the medical record is continually updated and modified, it is, in a sense, a living document. In terms of function, the medical record facilitates communication between providers, supports claims for reimbursement, and documents medical reasoning in the event of litigation, peer review, or medical board inquiry [32]. Thus, the medical record is simultaneously a medical, administrative, and legal document. The basic requirements for documentation in the medical record are generally prescribed by numerous entities including, but limited to, the Centers for Medicare & Medicaid Services (CMS) [33], the National Committee for

Quality Assurance (NCQA) [34], the Joint Commission [35], state statutes,[1] and also, hospital policies and medical staff bylaws.

The ownership of the patient's medical records is divided between the provider and the patient: the provider has ownership (or custody) of the physical patient records and chart, whereas the patient has ownership of the information contained therein. Thus, the safety and the integrity of the medical record is the responsibility of the custodian, institution, or provider. The minimum record retention rules for medical records is mandated by federal [37] and state laws, and also multiple regulatory agencies [38]. Clinicians must know, understand, and follow all applicable laws and regulations.

The Health Insurance Portability NAND Accountability Act of 1996 (HIPAA)

Overview of HIPAA

US Congress began to address concerns regarding the portability and renewability of health insurance in the 1970s starting with legislation such as the Employee Retirement Income Security Act (ERISA) of 1974 and the Consolidated Omnibus Reconciliation Act of 1985 (COBRA). The Federal Privacy Act of 1974 exemplified concerns regarding the inevitability of computerized information management and the associated security concerns associated with storage and transmission of sensitive information.

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by Congress in 1996 [39]. Broadly stated, the goals of HIPAA were to (1) increase the efficiency of electronic healthcare transactions; (2) ensure the continuity of employee's health insurance coverage after leaving an employer in the process of changing jobs; and (3) mandate widespread uniform adoption of privacy protection measures for ensuring the security of individually identifiable health information. Thus, HIPAA is a complex framework of regulations intended to facilitate portability of health data; reduce administrative costs by increasing efficiency through information technology (IT); maintain the integrity of electronically stored health data; and mandate the confidentiality of health information.

HIPAA is divided into five titles:

- Title I: HIPAA Health Insurance Reform/Access, Portability, and Renewability
  Requires employers and health plans to allow a medical insurance coverage to remain continuous despite pre-existing conditions; protects health insurance coverage for workers and their families when they change employment.
- Title II: HIPAA Administrative Simplification/Healthcare Fraud and Abuse

[1] See, for example, [36].

Requires the Department of Health and Human Services (HHS) to establish national standards for electronic healthcare transactions and national identifiers for providers (the National Provider Identifier; NPI), health plans (the Standard Unique Health Plan Identifier; HPID), and employers (the Standard Unique Employer Identifier; (EIN). It also addresses the security and privacy of health data. Adopting these standards will improve the efficiency and effectiveness of the nation's healthcare system by encouraging the widespread use of electronic data interchange in health care. Title II also addresses the security and privacy of health data and intended to prevent healthcare fraud and abuse.

- Title III: HIPAA Tax-Related Health Provisions

  Provides changes to health insurance laws and deductions for medical insurance and guidelines for pre-tax medical spending accounts.
- Title IV: Application and Enforcement of Group Health Plan Requirements

  Specifies conditions for group health plans regarding coverage of persons with preexisting conditions and modifies the continuation of coverage requirements.
- Title V: Revenue Offsets

  Includes provisions related to taxes affecting company-owned life insurance and to the treatment of individuals without US citizenship.

In the Federal Privacy Act, the federal government articulated the increasing importance and also the vulnerability of electronic data interchange (EDI) between business partners. Throughout the early stages of EDI, there was tremendous heterogeneity in the electronic and coding languages used, the information technology platforms, and the means of transmission. In healthcare, that lack of standardization was an obstacle to the evolution of the electronic medical record, access to health information, and the portability of health records. The Administrative Simplification provisions of HIPAA mandated the development of transaction and code sets to standardize the format of health information for storage, use, and EDI. HIPAA represented a uniform starting point for industry standardization of health information management and set the stage for the development of the electronic health/medical record (the EHR or EMR). The Institute of Medicine, in its 2001 report, "Crossing Quality Chasm: A New System for the 21st Century," [40] called for the creation of a national information infrastructure and for the increased adoption of information technology within the healthcare industry to facilitate access and to optimize quality and cost management, as well as quality and cost comparisons. Thus, HIPAA also sets the stage for a standardized data architecture, and information technology infrastructure allows the warehousing of healthcare data which would then facilitate quality comparisons, improve the quality of medical care, and facilitate the development of cost reduction strategies across the US healthcare system.

HIPAA privacy standards represent a national set of minimum basic protections. Noncompliance with the HIPAA Administrative Simplification regulations is enforced by the Centers for Medicare and Medicaid Services (CMS). Thus, in general, state laws contrary to HIPAA are preempted. "Contrary" means that it would be impossible for a covered entity to comply with both the state and federal

requirements or that the provision of state law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA. Therefore, HIPAA will preempt any contrary provision of any state law relating to written or electronic records. However, preemption may not apply if the state law: (a) is necessary to prevent fraud and abuse related to the provision of or payment for health care, (b) is necessary to ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation; (c) is necessary for state reporting on healthcare delivery or costs and is necessary for purposes of serving a compelling public health, safety, or welfare need and if a privacy rule provision is at issue and if the secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or, (d) has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802) or that is deemed a controlled substance by state law [41].

HIPAA was divided into three interrelated parts: (1) the privacy rule provisions which set security standards and policies for the way in which providers manage personally identifiable health information (PHI); (2) the security rule which governs relationships between healthcare business associates who necessarily exchange confidential medical information; and, (3) the enforcement rule which provides for the enforcement of all the Administrative Simplification rules.

The HIPAA Privacy Rule

The HIPAA Privacy Rule addresses the process by which covered entities acquire, store, and disclose individually identifiable health information. The Privacy Rule was published in 2000 and was subsequently modified in 2002.

The Privacy Rule [42] delineates national standards for the protection of individuals' medical records and other personal health information (PHI) regardless of the format; it applies to health plans, healthcare clearinghouses, and healthcare providers who conduct healthcare transactions electronically. The Privacy Rule mandates safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures of such information. The Privacy Rule was designed to (1) increase the level of patient control over the use of their medical records, (2) balance public health needs and responsibilities against information confidentiality, and (3) establish procedural safeguards to protect health information privacy. An individual's control over their PHI under HIPAA requires providers to (a) notify individual patients regarding the privacy rights and how their PHI is used through a process of adequate notice, (b) allow individuals the right to inspect and copy their medical records, (c) allow individuals to request amendments to their PHI record set, (d) receive an accounting of certain types of disclosures of their PHI, and (e) request the placement of restrictions on specific uses or disclosures of their PHI, with the exception of emergency treatment situations. Under HIPAA, patients also have a right to obtain and review a covered entity's "notice of privacy

practices." Individually identifiable health information includes many common identifiers such as name, address, birth date, and social security number. The Privacy Rule excludes employment records maintained by employers and educational institutions and other records subject to, or defined in, the Family Educational Rights and Privacy Act [43].

Definitions in HIPAA are essential since they represent legal terms of art (see Chap. 28: Anatomy of Healthcare Contracts: Pitfalls and Avoidance of Liability).

HIPAA defines the terms [44]:

- "Covered entity" to mean "(1) a health plan; (2) a health care clearinghouse; or, (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter."
- "Healthcare provider" to mean "a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business."
- "Health care" to mean "care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following: (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription."
- "Health information" to mean "any information, whether oral or recorded in any form or medium, that - (a) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (b) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to individual."
- "Protected health information" to mean "individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium (2). Protected health information excludes individually identifiable health information: (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232 g; (ii) In records described at 20 U.S.C. 1232 g(a) (4)(B)(iv); (iii) In employment records held by a covered entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years."
- "Individually identifiable health information" to mean "information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or

future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual."

- "Disclosure" to mean "the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information."
- "Electronic media" to mean:
  - (1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;
  - (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.
- "Business associate" to mean:
  - (1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:
    - (i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing;
    - (ii) or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.
  - (2) A covered entity may be a business associate of another covered entity.

– (3) Business associate includes:

  (i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.
  (ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.
  (iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

– (4) Business associate does not include:

  (i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.
  (ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of §164.504(f) of this subchapter apply and are met.
  (iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.
  (iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Health information is considered to be used when it is "shared" within a healthcare entity, and it is considered to be "disclosed" when it is shared outside that entity. Disclosure of confidential health information may be either required or permitted. A covered entity must disclose PHI (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their PHI and (b) to HHS in the event of compliance investigation or review or enforcement action [45] (*see* Chap. 12, The Implications of False Claims, Stark, and Anti-Kickback Laws). Covered entities are permitted, but not required, to disclose PHI, even absent an individual's authorization, in the following instances [46]:

(1) To the individual
(2) Treatment, payment, and healthcare operations:

Treatment is defined as "the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another." [47] *Payment* is defined to

address the "activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual." [47] *Healthcare operations* are defined to include any of the following activities: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity [47].

(3) Opportunity to agree or object:

Informal permission is obtained either explicitly, or through the operation of, circumstances that clearly give the individual the opportunity to agree, acquiesce, or object. These situations will occur in the case of facility directories, wherein healthcare facilities will maintain a directory of patients and their contact information. In such cases the facility or provider inquire about the individual by name, and providers may also disclose religious affiliation to clergy [48].

(4) Incident to an otherwise permitted use and disclosure

(5) Public interest and benefit activities:

The Privacy Rule permits use and disclosure of PHI, without an individual's authorization or permission, for 12 "national priority" purposes [49]:

(a) *Required by Law*: such as by statute, regulation, or court order [50].

(b) *Public Health Activities*: in the event of "(1) public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect; (2) entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and postmarketing surveillance; (3) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and (4) employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OHSA), the Mine Safety and Health Administration (MHSA), or similar state law" [51].

(c) *Victims of Abuse, Neglect, or Domestic Violence*.

(d) *Health Oversight Activities*: "such as audits and investigations necessary for oversight of the health care system and government benefit programs" [52].
(e) *Judicial and Administrative Proceedings*: "if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual or a protective order are provided" [53].
(f) *Law Enforcement Purposes*: Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances and subject to specified conditions:

i. "as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests;
ii. to identify or locate a suspect, fugitive, material witness, or missing person;
iii. in response to a law enforcement official's request for information about a victim or suspected victim of a crime;
iv. to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death;
v. when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and,
vi. by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime" [54].

Furthermore, the authorization to use or disclose psychotherapy notes must be specific with some specific exceptions, including, "to avert a serious and imminent threat to public health or safety…" [55].

(6) Limited data set for the purposes of research, public health, or healthcare operations: used and disclosed for research, healthcare operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set. HIPPA makes exceptions regarding the use of PHI for research. HIPAA defines "research" as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge" [47]. HIPAA regulations protect only that health information which is individually identifiable (PHI). Generally, appropriately de-identified patient data can be used or shared without restrictions in situations such as clinical research, organizational strategic planning, and epidemiologic research. De-identified data refers to aggregate statistical data stripped of individual identifiers.

In addition, even the use of PHI may be used internally within institutions (covered entities) to facilitate or optimize healthcare operations, provided that the information is not disseminated. Thus, PHI may generally be used internally within

organizations, without authorization, in the course of operational, financial, or strategic planning, competency assurance, credentialing and accreditation, medical reviews, or legal services and to manage compliance programs.

HIPAA also differentiates between the terms "consent" which refers to a broad general permission that is granted by the individual to a "covered entity" to use or disclose PHI for treatment, payment, or healthcare operations and "authorization" which refers to more specific and detailed permission to share PHI. The request and the consent and authorization to release individually identifiable health information for any purpose must therefore be to express, in plain language and specify the information to be disclosed, the person(s) disclosing and those receiving the information, the expiration of the consent to disclose, and the right to revoke in writing. Authorization for the release of PHI must be documented in writing. A sample authorization form is included at the end of this chapter.

Arguably, HIPAA makes allowances for professional ethics and best judgment may guide the permissive uses and disclosures of PHI. Clinicians must often access PHI medical in critical and emergency treatment situations where a documented consent cannot be obtained in a timely fashion. In such cases, the provider must nonetheless obtain consent as soon as it is reasonably possible to do so. Thus, the Privacy Rule does not absolutely mandate that information not be shared without consent in all circumstances; rather, that disclosure of information should be "incident to" medical justification. Permissible reasonable use or disclosure of PHI therefore permitted in degrees, as long as the provider uses reasonable safeguards to inappropriate disclosure, and that information shared is limited to the "minimum necessary" information necessary under the clinical circumstances, often referred to as the "minimum necessary" standard for PHI disclosure.

The HIPAA Security Rule

The HIPAA Security Rule, published in 2003, mandates administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI (ePHI). Thus, the Security Rule specifically applies to and protects a subset of medical record information that is covered in the Privacy Rule; the Security Rule applies to individually identifiable health information that a covered entity creates, receives, maintains, or transmits in electronic form. The Security Rule defines "confidentiality" to mean that e-PHI is not made available or disclosed to unauthorized persons. The Security Rule applies to health plans, healthcare clearinghouses, and to any healthcare provider who transmits health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities"); the HITECH Act of 2009 (see below) expanded the responsibilities of "business associates" under the HIPAA Security Rule. Failure to meet security standards risks both civil and criminal penalties under HIPAA but also incurs potential civil liability under private causes of action initiated by plaintiffs, or their representatives, under state tort, privacy contract, and consumer protection laws and also under state heath oversight statutes.

A key mandate of the HIPAA Security Rule is the mandate for a program of ongoing risk analysis and a program for risk management. Ideally, the risk analysis and management program of any institutions should be included in its HIPAA compliance plan. An entity's security and compliance program are subject to federal scrutiny, on demand, at any time. The risk analysis process should include, at least, (a) an assessment and evaluation of the likelihood and impact of potential risks to e-PHI; (b) the implementation of appropriate security measures to address the risks identified in the risk analysis; (c) documentation of the rationale for choosing the security measures adopted; and (d) a program of continuous, reasonable, and appropriate security assessment [56]. Under the Security Rule, the requisite safeguards to ensure the integrity of ePHI are (1) administrative safeguards; (2) physical safeguards; and (3) technical safeguards.

Administrative safeguards are those administrative actions and policies and procedures which are enacted to protect eHPI. These safeguards focus on the policies and procedures designed to prevent, detect, contain, and correct security violations. The general elements of administrative safeguards, under HIPAA, are (1) the designation of a security official who is responsible for developing and implementing its security policies and procedures; (2) access management through policies and procedures for authorizing "role-based access" within an entity; (3) workforce training and management through authorization and supervision, and policies for sanctions against workforce members who fail to comply with, or violate, security policies and procedures; and (4) periodic assessment of the efficacy of existing security policies and procedures [57]; these may include, for example, audit logs, access reports, and security incident tracking reports.

The Security Rule also includes a contingency plan as a standard under administrative safeguards. Entities must protect the integrity of ePHI through contingency plans designed to maintain access to potentially critical ePHI required for medical care in the event of a catastrophe. Contingency planning is often managed under business continuity planning (BCP) and disaster recovery planning (DRP) which are the overall processes to ensure data backup, disaster recovery, emergency operations [58]. Additionally, entities must develop and implement (1) procedures and policies regarding periodic testing and revision of contingency plans and (2) an assessment of the relative criticality of specific data management applications.

Physical safeguards include (1) limitation of physical access to the facilities while ensuring authorized access as needed and (2) training, education, and policies and procedures which specify proper use of and access to workstations and electronic media. Covered entities must also develop and implement policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media [59]. Entities must also be able to timely identify and respond to suspected or known security incidents, mitigate the potential harm of known security, and develop a system to document the nature of security incidents and their impact. In addition, good monitoring of the efficacy of physical safeguards might include (a) regular updates, education, and reminders; (b) procedures for guarding against, detecting, and reporting malicious software such as malware, hacking, Trojan horses, or viruses; (c) continuous monitoring of failed log-in attempts and password

discrepancies; and (d) policies and schedules for creating, changing, and safeguarding passwords.

Technical safeguards include (1) technical policies and procedures for the restriction of access to authorized persons; (2) audit controls; (3) integrity controls; and (4) transmission security while e-PHI is transmitted over an electronic network [60].

The HIPAA Enforcement Rule

Enforcement of the Privacy Rule became effective in 2003; and the enforcement of the Security Rule became effective in 2005. The Office for Civil Rights (OCR), within HHS, is responsible for investigating and enforcing the Privacy and Security Rules; and OCR refers to cases and may collaborate with the Department of Justice (DOJ) to investigate criminal violations of HIPAA. In general, the OCR investigates complaints; however, the OCR may also conduct random compliance reviews to review compliance plans. A complaint must allege an activity which, if proven, would violate the Privacy or Security Rule. Such complaints must be filed within 180 days of when the person submitting the complaint knew or should have known about the alleged violation of the Privacy or Security Rule.

In general, a HIPAA violation occurs when a HIPAA-covered entity fails to adhere to, or violates, one or more of provisions of the HIPAA Privacy, Security, or Breach Notification Rules. CMPs for HIPAA violations are assessed based on a tiered civil penalty structure (Table 13.1):

- Tier 1: The covered entity was unaware of the HIPAA violation and, through reasonable due diligence, could not have known of a HIPAA violation.
- Tier 2: Through the exercise of its reasonable due diligence, the covered entity knew or reasonably should have known of, but could not have reasonably prevented a HIPAA violation.
- Tier 3: Willful neglect of HIPAA Rules with correction of the violation within 30 days of discovery.
- Tier 4: Willful neglect of HIPAA Rules, where no efforts have been made to correct the violation within 30 days of discovery.

For the purposes of HIPAA violations, the following definitions apply:

1. “Reasonable cause” is defined as “an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.”
2. “Reasonable diligence” is defined as “the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.”
3. ‘Willful neglect’ is defined to mean “conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated” [61].

Table 13.2 Criminal penalties under HIPAA

Culpability category	Penalty
Knowingly	$ 50,000 + 1 year prison
False pretenses	Up to $ 50,000 + 5 years prison
Intent for monetary gain	Restitution + up to $ 250,000 + 10 years prison

In addition to CMPs, HHS has the authority to exclude entities and/or providers from participation in federally funded payment programs, such as Medicare and potentially Medicaid.

Criminal actions for HIPAA violations are investigated and prosecuted by the DOJ. For the purposes of criminal prosecutions under HIPAA, the term "knowingly" requires only that the entity has knowledge of the actions that constitute an offense; there is no requirement that the entity actually or specifically know that the actions are in violation of the HIPAA statute.

There are three tiers of criminal penalties for HIPAA (Table 13.2):

- Tier 1: Reasonable cause or no knowledge of violation – a maximum of 1 year in jail
- Tier 2: Obtaining PHI under false pretenses – a maximum of 5 years in jail
- Tier 3: Obtaining PHI for personal gain or with malicious intent – a maximum of 10 years in jail

In addition to HIPAA violations through the unauthorized disclosure of ePHI, the OCR may impose CMPs for HIPAA noncompliance, in instances where no breach of PHI occurred but the entity has failed to develop and implement a compliance program. Key compliance program risks are (1) failure to complete a comprehensive, organization-wide risk assessment and (2) failure to execute business associate agreements (BAAs).

Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 [63] was enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA) [64]. HITECH built upon the foundation of HIPAA to expand the adoption of, and the leverage of information (as opposed to data entry) capabilities of EHRs, together with enhanced access, privacy, and security provisions for PHI management (Table 13.3).

Within the HHS, two agencies, the CMS and the Office of the National Coordinator for Health Information Technology (ONC), collaborated to coordinate the operationalization of the HITECH Act, together defining meaningful use criteria and EHR certification criteria. EHR certification criteria (defined by the ONC) specified the requisite functional (the what) criteria for a certified EMR, whereas the meaningful use criteria (defined by CMS) specified the operational (the how) criteria of a certified EHR system.

Table 13.3 Key provisions of the HITECH Act relating to HIPAA privacy and security provisions

Area of regulation	Provision
Civil monetary penalties	Increase in the minimum penalty for each violation of HIPAA rules; increasing to up to $50,000 per violation and a maximum of $1.5 million for all annual repeat violation of the same provision
Use and disclosure of PHI	Prohibits the sale of PHI without a signed authorization
Breach notification	Mandatory HIPAA/PHI breach notification requirements imposed on covered entities and business associates
Business associate liability	Application of HIPAA compliance requirements to business associates
Meaningful use	

HITECH Breach Reporting Requirement

The first rule within HITECH, published by the HHS OCR in 2009, addressed notification requirements in the event of a breach of unsecured PHI and mandated the notification of affected individuals in the event that a security breach when "unsecure PHI" is disclosed or used for an unauthorized purpose [65]. A breach is defined as an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. The breach reporting requirement requires healthcare providers and other HIPAA covered entities to promptly notify affected individuals of a breach, as well as the HHS secretary and prominent media outlets, in the form of a press release, to media serving the state or jurisdiction in cases where a breach affects more than 500 individuals [66].

There are three exceptions to the definition of "breach":

(1) The unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.
(2) The inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate or organized healthcare arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
(3) If the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information [67].

Under HITECH, "unsecured PHI" essentially means "unencrypted PHI."

Meaningful Use

The second rule, published by the HHS CMS in 2009, addressed incentive payments available under the Medicare and Medicaid programs for hospitals, physicians, and other healthcare providers who qualified as "meaningful users" of EHRs [68]. HITECH provided financial incentives to "eligible professionals" for the meaningful use of certified qualified electronic health records (EHRs) beginning in 2011 and penalties for failure to achieve meaningful use after 2015 [69].

Through focusing on the effective use of EHRs with certain capabilities, the HITECH Act makes clear that the adoption of records is not a goal in itself: it is the use of EHRs to achieve health and efficiency goals that matter. HITECH's incentives and assistance programs seek to improve the health of Americans and the performance of their healthcare system through "meaningful use" of EHRs to achieve five health care goals:

- To improve the quality, safety, and efficiency of care while reducing disparities
- To engage patients and families in their care
- To promote public and population health
- To improve care coordination
- To promote the privacy and security of EHRs [70]

"Meaningful Use" incentive payments were conditioned by CMS upon the demonstration of the (1) use of certified EHR technology in a demonstrably meaningful manner, for example, e-prescribing; (2) the use of certified EHR technology so as to facilitate the exchange of electronic health data and information so as to improve the quality of healthcare, such as promoting care coordination; and (3) the use of certified EHR technology to report clinical quality measures (CQM) and other measures selected by the HHS secretary [71]. The Meaningful Use program consisted of three stages:

- Stage 1 Meaningful Use established basic requirements for the electronic capture of clinical data, including providing patients with electronic copies of their PHI.
- Stage 2 Meaningful Use expanded on Stage 1 criteria with a focus on advancing clinical processes and ensuring that the meaningful use of EHRs supported the aims and priorities of the national quality strategy. Stage 2 criteria encouraged the use of CEHRT for continuous quality improvement at the point of care and the exchange of information in the most structured format possible.
- Stage 3 Meaningful Use established in 2017, focused on using CEHRT to improve health outcomes [72].

In order to comply with meaningful use of certified EHR technology as defined by CMS, providers must report on a combination of required core objectives, objectives selected from a menu set, and reporting of CQMs as specified by HHS [73]. In 2018, eligible healthcare professionals (EPs) or eligible clinicians (ECs) who had

been participating in the Medicare Promoting Interoperability Program (MPIP) were required to report using the quality payment program (QPP) measures; also in 2018, CMS renamed the EHR incentive programs as the promoting interoperability programs.

Certification Criteria for EHR Technology

The third rule, published by the HHS ONC, developed certification criteria for EHR technology. The ONC is charged with the development and coordination of a nationwide health information technology (HIT) strategy and policy and the promotion of a nationwide HIT infrastructure for the management of electronic health information. The ONC was created by the HITECH Act and is a division HHS was created by Executive Order in 2004.

The third rule identified the functional and technical capabilities that the EHR technology and systems must possess:

> …certification criteria establish the required capabilities and specify the related standards and implementation specifications that serve as an electronic health record (EHR) technology will need to include to, at a minimum, support the achievement of meaningful use Stage 1 by eligible professionals, eligible hospitals, and/or critical access hospitals…under the Medicare and Medicaid EHRs Incentive Programs. [74]

The following definitions were applied to certified EHR technology:

> (1) A Complete EHR that meets the requirements included in the definition of a Qualified EHR and has been tested and certified in accordance with the certification program established by the National Coordinator as having met all applicable certification criteria adopted by the Secretary; or
> (2) A combination of EHR Modules in which each constituent EHR Module of the combination has been tested and certified in accordance with the certification program established by the National Coordinator as having met all applicable certification criteria adopted by the Secretary, and the resultant combination also meets the requirements included in the definition of a Qualified EHR.

Where a "Complete EHR means EHR technology that has been developed to meet, at a minimum, all applicable certification criteria adopted by the Secretary" [74].

Business Associates and the Privacy and Security Provisions of HITECH

The privacy and security provisions of HIPPA were directly applicable to "covered entities," defined in HIPAA as healthcare payers, providers, and clearinghouses; business associates were indirectly, but not directly, bound to the HIPAA provisions. In HIPAA, the Privacy Rule required nonemployee "business associates"

whose relationships with "covered entities" required the sharing of PHI to establish a "chain of trust partner agreement" now referred to as a "business associate agreement." HIPAA required the "business associate" to:

(1) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the "covered entity's EHPI
(2) Ensure that its agents, and subcontractors, to whom it provides EHPI agree to implement reasonable and appropriate safeguards to protect it
(3) Report to the covered entity any security incident of which it becomes aware
(4) Ensure that the contract authorizes unilateral termination of the agreement if the business associate has violated a material contractual term

Although the BAA was less prominent in HIPAAA, the HITECH Act directly applied HIPAA provisions directly to business associates, mandating that covered entities establish contractual agreements with every business associate, known as business associate agreements (BAAs). Failure to have BAAs is considered a serious compliance violation under HITECH and cause for OCR disciplinary proceedings.

HIPAA Violation Fines Can Also Be Issued by State Attorneys General

Under the HITECH Act as of 2009, state attorneys general (SAGs) are empowered to hold HIPAA-covered entities accountable for the exposure of the PHI of state residents and initiate separate civil actions for PHI disclosure violations [75]. HITECH extends HIPAA violation fines to the states with a minimum fine of $100 per violation to a maximum level of $25,000 per violation category, per calendar year. Furthermore, a covered entity that sustains a data breach affecting residents of multiple states may be fined for HIPAA violation penalties by SAGs in multiple states. OCR developed HIPAA enforcement training in order to educate and train SAG and their staff enforce the HIPAA Privacy and Security Rules. Enhanced collaboration and enforcement coordination between the OCR and the SAGs will allow the OCR to assist SAG in the exercise of this new enforcement authority through the sharing of breach information regarding pending or concluded OCR actions against covered entities or business associates related to SAG investigations, and the OCR will also provide SAGs guidance regarding the HIPAA statute, the HITECH Act, and the HIPAA Privacy, Security, and Enforcement Rules as well as the Breach Notification Rule as needed to effectively prosecute these cases on a state level. The implication to providers is that the HITECH Act increases the potential liability for healthcare information privacy breaches by an additional layer, above and beyond the HIPAA and HITECH CMP fines, state disciplinary procedures, and private civil causes of action, potential criminal liability, and potential CMS exclusion.

References

1. Merriam-Webster Dictionary. Available online at: https://www.merriam-webster.com/dictionary/privacy.
2. Merriam-Webster Dictionary. Available online at: https://www.merriam-webster.com/legal/right%20of%20privacy.
3. Griswold v. Connecticut. 381 U.S. 479. (1965).
4. Olmstead v. U. S. 277 U.S. 438. (1928). Justice Brandeis's dissent at 61, 72, and 73.
5. Warren S, Brandeis LD. The right to privacy. Harvard Law Rev. 1890;4(193)
6. Prosser Restatement of the Law, Second, Torts, § 652. The American Law Institute. 1977.
7. Prosser, *supra* at § 652B Intrusion Upon Seclusion.
8. Prosser, *supra* at § 652C Appropriation of Name or Likeness.
9. Prosser, supra at § 652D Publicity Given to Private Life.
10. Bruce A. McKenna, False Light: Invasion of Privacy, 15 Tulsa L. J. 113 (2013).
11. Urs Gasser. Recoding privacy law: reflections on the future relationship among law, technology, and privacy. Harvard Law Rev. 2016;130(2)
12. Becker M. Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy. Ethics Inform Technol. 2019;21:307–17.
13. Szalados JE. Digital distraction and legal risk. In: Bertman S, Papadakos PJ, editors. Distracted doctoring: returning to patient-centered care in the digital age. Cham: Springer; 2017.
14. Edna Selan Epstein. The attorney-client privilege and the work-product doctrine. American Bar Association, Section of Litigation. Chicago. 2017.
15. Prichard v. United States, 181 F.2d 326 (6th Cir. 1950), aff'd 339 U.S. 974, 70 S. Ct. 1029, 94 L. Ed. 1380 (1950).
16. United States v. Grand Jury Investigation, 401 F. Supp. 361 (W.D. Pa. 1975).
17. Cathryn MS. The application of the attorney-client privilege to communications between lawyers within the same firm: Evaluating United States v. Rowe, 30 ARIZ. ST. L. J. 859, 859. 1998.
18. 8 Wigmore on Evidence §2292, at 554 (McNaughton ed. 1961).
19. Togstad v. Vesely, 291 N.W.2d 686 (1980).
20. Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).
21. Paul RR. Attorney-client privilege: continuing confusion about attorney communications, drafts, pre-existing documents, and the source of the facts communicated, 48 AM. U. L. REV. 967, 969–70. 1999.
22. The Editors of Encyclopaedia Britannica. Hippocratic oath. Available online at: https://www.britannica.com/topic/Hippocratic-oath.
23. Witherell v. Weimer, 421 NE2d 869 (1981).
24. The Privacy Act of 1974 (Pub.L. 93–579, 88 Stat. 1896, enacted December 31, 1974. 5 U.S.C. § 552a.
25. U.S. Department of Justice. Office of Privacy and Civil Liberties. Overview of the Privacy Act of 1974. Online at: https://www.justice.gov/opcl/introduction.
26. Joint Commission on Accreditation of Healthcare Organizations. Medical Record Services (MR). Accreditation Manual for Hospitals. Chicago; 1990.
27. Thacker SB. Historical development. In: Lee LM, Teutsch SM, Thacker SB, St. Louis ME, editors. Principles and practice of public health surveillance. 3rd ed. New York: Oxford University Press; 2010. p. 1–17.
28. Lee LM, Heilig CM, White A. Ethical justification for conducting public health surveillance without patient consent. Am J Public Health. 2012;102(1):38–44.
29. Tarasoff v. Regents of the University of California. S.F. 23042. December 23, 1974.
30. Tarasoff v. Regents of University of California (1976) 17 Cal.3d 425, 434–436, 131 Cal.Rptr. 14, 551 P.2d 334.
31. Kachigian C, Felthous AR. Court responses to Tarasoff statutes. J Am Acad Psychiatry Law. 2004;32(3):263–73.

32. Szalados JE. Health information privacy and HIPPA: the health insurance portability and accountability act. Curr Rev Clin Anesth. 2004;25(1):3–14.
33. CMS. Complying with Medical Record Documentation Requirements. Available online at: https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/CERTMedRecDoc-FactSheet-ICN909160.pdf.
34. NCQA. Guidelines for Medical Record Documentation. Available online at: https://www.ncqa.org/wp-content/uploads/2018/07/20180110_Guidelines_Medical_Record_Documentation.pdf.
35. HCPro. Know the JCAHO's ongoing records review requirements. Available online at: https://www.hcpro.com/HIM-53615-865/Know-the-JCAHOs-ongoing-records-review-requirements.html.
36. New York Codes, Rules and Regulations. Title 10, Chapter V, Subchapter A, Article 2, Part 405, Section 405.10 - Medical records. Available online at: https://regs.health.ny.gov/content/section-40510-medical-records. 42 CFR § 485.638.
37. Condition of participation: Medical record services. 42 CFR § 482.24(b)(1) and 42 CFR § 485.638(c); Conditions of participation: Clinical records. 42 CFR § 485.638.
38. *See, for example*, American Health Information Management Association, Retention and Destruction of Health Information. Available online at: https://library.ahima.org/PB/RetentionDestruction#.XvDx6mhKiUk.
39. Health Insurance Portability and Accountability Act of 1996. Pub. L. No. 104–191, 100 Stat. 1396; as codified at 45 CFR § 160 et seq. (2000); and as amended.
40. Institute of Medicine. Crossing the quality chasm: a new system for the 21st century. Washington DC: National Academy Press; 2001.
41. HIPAA. 45 C.F.R. § 160.203; and 45 C.F.R. § 160.202.
42. HIPAA. 45 CFR Part 160 and Subparts A and E of Part 164. The Privacy Rule; and as updated; *See also* US Department of Health and Human Services, HHS. The HIPAA Privacy Rule. Available online at: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.
43. Family Educational Rights and Privacy Act 20 U.S.C. §1232g.
44. HIPAA. 45 CFR §160.103. See supra. Definitions. “Health Information”.
45. HIPAA. 45 C.F.R. § 164.502(a)(2).
46. HIPAA. 45 C.F.R. § 164.502(a)(1).
47. HIPAA. 45 C.F.R. § 164.501.
48. HIPAA 45 C.F.R. § 164.510(a).
49. HIPAA. See 45 C.F.R. § 164.512.
50. HIPAA. 45 C.F.R. § 164.512(a).
51. HIPAA. 45 C.F.R. § 164.512(b).
52. HIPPA. 45 C.F.R. § 164.512(d).
53. HIPAA. 45 C.F.R. § 164.512(e).
54. HIPPA. 45 C.F.R. § 164.512(f).
55. HIPAA. 45 C.F.R. § 164.501. “Psychotherapy notes” means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the of the individual’s medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. See also HIPAA. 45 C.F.R. § 164.508(a)(2).
56. HIPAA [8] 45 C.F.R. § 164.306(b)(iv); 45 C.F.R. § 164.308(a)(1)(ii)(B); 45 C.F.R. § 164.306(d)(3)(ii)(B)(1); 45 C.F.R. § 164.316(b)(1); and 45 C.F.R. § 164.306(e).
57. HIPAA. 45 C.F.R. § 164.308(a)(2); 45 C.F.R. § 164.308(a)(4)(i); 45 C.F.R. § 164.308(a)(3) & (4); 45 C.F.R. § 164.308(a)(5)(i); 45 C.F.R. § 164..308(a)(1)(ii)(C); and 45 C.F.R. § 164.308(a)(8).
58. HIPAA. 164.308(a)(7)(i); 164.308(a)(7)(ii)(A)-(E).

59. HIPAA. 45 C.F.R. § 164.310(a); 45 C.F.R. §§ 164.310(b) & (c); and 45 C.F.R. § 164.310(d).
60. HIPAA. 45 C.F.R. § 164.312(a); 45 C.F.R. § 164.312(b); 45 C.F.R. § 164.312(c); 45 C.F.R. § 164.312(e).
61. HIPAA 45 CFR §160.401 Definitions.
62. HIPAA. 45 CFR §160.404 Amount of a civil money penalty.
63. Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009) (full-text), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq.
64. American Recovery and Reinvestment Act (ARRA) of 2009, Pub. L. No. 111-5, 123 Stat. 115, 516 (Feb. 19, 2009).
65. U.S. Department of Health and Human Services, Breach Notification for Unsecured Protected Health Information, Interim final rule with request for comments. 45 CFR Parts 160 and 164, Federal Register 74, August 24, 2009; p. 42740.
66. HHS. HITECH Breach Notification Interim Final Rule. 2013. Available online at: https://www.hhs.gov/hipaa/for-professionals/breach-notification/laws-regulations/final-rule-update/hitech/index.html.
67. HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414. See also, Breach Notification Rule. HHS. Available online at: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.
68. Medicare and Medicaid Programs: Electronic Health Record Incentive Program. Federal Register 75, January 13, 2010; p. 1844. The proposed regulations will be located mainly at new part 495 of title 42 of the Code of Federal Regulations. Amendments are also proposed for parts 412, 413, and 422 of title 42.
69. HITECH Act of 2009, 42 USC sec 139w-4(0)(2) (February 2009), sec 13301, subtitle B: Incentives for the Use of Health Information Technology.
70. CMS. Newsroom. CMS and ONC final regulations define meaningful use and set standards for electronic health record incentive program. 2010. Available online at: https://www.cms.gov/newsroom/fact-sheets/cms-and-onc-final-regulations-define-meaningful-use-and-set-standards-electronic-health-record.
71. ARRA Title IV Subtitle A § 4101(a) (adding new section 1848(o)(2)(A) to the Social Security Act), 42 U.S.C.A. § 1395w-4 (West, Westlaw through March 2010).
72. Centers for Disease Control and Prevention. CDC. Public Health and Promoting Interoperability Programs (formerly, known as Electronic Health Records Meaningful Use). 2019. Available online at: https://www.cdc.gov/ehrmeaningfuluse/introduction.html.
73. Centers for Medicare and Medicaid services. Medicare and Medicaid EHR incentive program: Meaningful use stage 1 requirements overview. 2010. Available online at: https://www.cms.gov/EHRIncentivePrograms/Downloads/MU_Stage1_ReqOverview.pdf.
74. Health information technology: initial set of standards, implementation specifications, and certification criteria for electronic health record technology. Final rule. Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services. Fed Regist. 2010; 75(144):44589–654.
75. HITECH Act (Section 13410(e) (1)).