Whether the Health Insurance Portability Accountability Act has Become Obsolete in the Nation’s Movement Towards Health Information Technology?

Radhika Vemula

Available at: https://works.bepress.com/radhika_vemula/1/
WHETHER THE HEALTH INSURANCE PORTABILITY ACCOUNTABILITY
ACT HAS BECOME OBSOLETE IN THE NATION’S MOVEMENT TOWARDS
HEALTH INFORMATION TECHNOLOGY?

Information technology promises many benefits to the health care sector by
improving quality and lowering the costs of health care. However, the prospect of storing
health information in electronic form raises concerns about patient privacy and data
security. Although information technology allows the use of advanced technology to
limit access to health information, it also introduces new vulnerabilities, such as access
by unauthorized users. Unless proper controls and adequate laws are in place, health care
organizations may be reluctant to adopt health information technology and patients
reluctant to share information, undermining the provision of care. This paper outlines the
evolution of privacy laws in America leading up to the enactment of the Health Insurance
Portability Accountability Act of 1996 (HIPAA), addresses why HIPAA lacks the ability
to keep up with emerging technologies in health care, and recommends the actions
Congress must take in expanding HIPAA to protect personal health information in the
twenty-first century.

I. INTRODUCTION

The entire health care system is built upon the willingness of individuals to share
the most intimate details of their lives with their health care providers.1 Some of the most
sensitive and personal information about an individual is their medical information, and
one cannot be expected to share such details unless they have confidence that the
information will not be used or shared inappropriately. For example, the medical files of

1 Furrow, Greaney, Johnson, Jost, & Schwartz, Health Law, Cases, Materials and
AIDS/HIV patients contain everything from symptoms and lab results to the diagnosis – AIDS/HIV status. Any unwanted access to, use, or disclosure of medical records could trigger rejection from their family and friends, loss of employment or clients, loss of income, discrimination, quarantine and the like.\(^2\) The relationship between a patient and a clinician is based on trust, and without full access to the most intimate details, the physician cannot adequately treat the patient. Privacy violations reduce consumers’ trust in the health care system and a loss of faith can impede the quality of the health care they receive.\(^3\)

Since the fourth century B.C., physicians have abided by the Hippocratic Oath which binds them to keep secret the information they learn from patients during the course of providing care. The growing use of information technology within the health care sector demands that issues of patient privacy and data security again be analyzed to ensure that policies, practices, and procedures for handling health information account for vulnerabilities in current systems.\(^4\) As health care organizations collect, process, and store more health information in computerized form and use both private and public telecommunications systems to transmit health information between different entities, organizations must ensure that adequate mechanisms are in place to protect the information.\(^5\)

Recent mishaps and growing litigation regarding the unauthorized disclosure of medical records demonstrate that a patchwork of applicable statutes, common law, and


\(^3\) Furrow, supra note 1, at 339.


\(^5\) *Id.*
constitutional law are inadequate to protect one’s private information and lack the deterrent effect necessary to prevent a breach. According to the Los Angeles Times, children’s psychological records from clinics across several states were accidentally posted by the University of Montana on the Internet.\(^6\) These files contained information on attention deficits, depression, schizophrenia, and other mental disorders, as well as complete names, ages, and, in some cases, the patients’ addresses and schools. This disclosure follows on the heels of a major health plan accidentally sending confidential health data by e-mail to the wrong plan members. In numerous other instances, employees of health agencies, plans and care providers have engaged in a variety of egregious practices, such as sharing copies of health data with a patient’s ex-husband, selling celebrities’ health records, and cross-listing cancer patients with borrowers of callable loans.\(^7\) These examples emphasize the need to implement health technology policies and procedures for electronic data interchange, privacy, and security, for all health information regardless of the applicability of HIPAA in a given case.\(^8\)

II. EXISTING FEDERAL AND STATE PROTECTIONS FOR HEALTH

The privacy and security of health information is influenced by many factors that operate at the public policy level. In the United States, protection of health information is generally divided between coverage for record systems operated by federal or state government agencies and record systems operated by the private sector.\(^9\) State health record laws generally define the types of information considered confidential and the

---

\(^7\) Id.
\(^8\) Id.
\(^9\) National Research Council, supra note 4.
circumstances under which health information can be shared without patient consent. Records held by the private sector are covered under a number of limited laws targeted at specific industries.\textsuperscript{10} At the federal level, data protection measures are found in constitutional law, the Privacy Act of 1974, and a few statutes that regulate narrow areas of data use. The hodgepodge of privacy laws and regulations established in the United States do not constitute adequate protection of one’s health information because they are limited in scope as most health data resides outside these protections.

\textbf{A. State Protections of Health Information}

At the state level, measures for protecting health information include state common law, state constitutional law, and state statutes. The “clear modern consensus of the case law” is to recognize the breach of confidentiality tort, which is premised on the existence of a fiduciary relationship between physician and patient.\textsuperscript{11} Common law tort remedies such as intrusion upon seclusion or public disclosure of private facts may also give rise to an invasion of privacy claim.\textsuperscript{12} State constitutional law has sometimes been interpreted as setting limits on the collection and dissemination of health data.\textsuperscript{13} Although state regulation is extensive in its protection, the practice and administration of modern medicine takes place on the interstate level\textsuperscript{14} making the varying state solutions

\begin{footnotesize}
\begin{enumerate}
\item National Research Council, supra note 4.
\item Cal. Const. art. I, §1.
\item Physicians attend medical school in one state, complete a residency in another state, and practice in another state; also, telemedicine is rapidly developing the application of clinical medicine where medical information is transferred via telephone, the Internet or
\end{enumerate}
\end{footnotesize}
to data protection unmanageable. Statutes do not exist in all states, are not uniform across states, and mostly do not address the flows of information to secondary users, such as laboratories, pharmacies, schools, public health officials, researchers, insurers, and other individuals and institutions. Finally, statutes do not address the responsibilities of third-party payers in handling health information, nor do they impose rules on the use of health information by secondary users of the data.

The breach of confidentiality tort requires that the patient be in a professional or contractual relationship with the person responsible for the wrongful disclosure. In *Humphers v. First Interstate Bank of Oregon*, a physician revealed the identity of the birth mother to a daughter who had been given up for adoption. The court held that the physician was liable for failing to keep a confidence under the breach of confidentiality. In *Biddle v. Warren*, a law firm entered into an arrangement with a hospital whereby medical records of patients with unpaid bills were disclosed for the purpose of obtaining information regarding eligibility for Social Security Insurance benefits. The hospital released the data to the law firm without obtaining the consent of the patients. The court held that not only was there a viable breach of confidentiality claim against the hospital, but also, the firm could be liable for inducing such a breach by proposing the arrangement.

---

18 Id.
The rule of confidentiality does not work nearly as well in a modern information society. A traditional breach of confidentiality action provides a remedy in the case of disclosure by a physician, but does not apply to disclosures made by downstream users. Past thinking assumed a paper or automated record was created and protected by the provider, but health data in the era of electronic information is based only in small part on the physician-patient relationship, and anyone with system access can call up a patient record on the screen with a click of the mouse. The breach of confidentiality tort has been viewed as unable to address the problems caused by the widespread dissemination of electronic health information among “downstream” users not in a relationship of confidentiality with the injured person. Since location has less meaning in an electronic world, protecting privacy requires attaching protection to the health record itself, rather than to the institution that generates it.

Some courts have recognized claims under the common law right of privacy. In the Estate of Berthiaume v. Pratt, a doctor attempted to take photographs of his patient, who was dying of cancer of the larynx. The patient raised a clenched fist and tried to

20 HIPAA’s Privacy Rule attempts to close this gap in the common law by requiring covered entities to sign a business associate contract.
21 This criticism of the breach of confidentiality tort was first made in the seminal 1890 law review article by Louis D. Brandeis and Samuel D. Warren, entitled The Right to Privacy, 4 Harv. L. Rev. 193 (1890): So long as these circumstances happen to present a contract upon which such a term can be engrafted by the judicial mind, or to supply relations upon which a trust or confidence can be erected, there may be no objection to working out the desired protection through the doctrines of contract or of trust. But the court can hardly stop there. The narrower doctrine may have satisfied the demands of society at a time when the abuse to be guarded against could rarely have arisen without violating a contract or a special confidence; but now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation.
22 Gostin, supra note 19.
remove his head from the camera’s range. The patient died later that day. The court held that the patient had a claim for intrusion upon seclusion because the doctor did not have the right, against the patient’s wishes, to complete his photographic record by taking pictures of the patient in his dying hours.\textsuperscript{23} Some courts have found that the disclosure of medication information can give rise to a claim for public disclosure of private facts. \textit{In Urbaniak v. Newtown}, the court held that the disclosure of a patient’s HIV status was clearly a “private fact” of which the disclosure may “be offensive and objectionable to a reasonable [person] of ordinary sensibilities.”\textsuperscript{24} In \textit{Doe v. Mills}, a group of abortion protestors held up large signs displaying the names of the plaintiffs outside the abortion clinic where they were getting abortions. The court held that the plaintiffs could bring a claim for public disclosure since abortion concerns matters of sexual relations and medical treatment, both of which are regarded as private matters.\textsuperscript{25}

Although courts have recognized some common law torts, the invasion of privacy theories are of limited use for medical record disclosures because they are limited in the context of personal health information.\textsuperscript{26} Most courts have found that to establish a claim for public disclosure of private records the plaintiff must show a widespread disclosure to the public, which will not occur in most cases involving the release of health information.\textsuperscript{27} Another restriction of the public disclosure tort is the requirement that the

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{23} \textit{Estate of Berthiaume v. Pratt}, 365 A.2d 792 (Me. 1976).
\item \textsuperscript{25} \textit{Doe v. Mills}, 536 N.W.2d 824 (Mich. App. 1995).
\item \textsuperscript{26} Restatement (Second) of Torts, § 652D supports this.
\item \textsuperscript{27} \textit{Porten v. Univ. of San Francisco}, 64 Cal. App.3d 825, 828-829, 134 Cal. Rptr. 839, 841 (Cal.App. 1 Dist. 1976). For criticisms of the requirement of widespread publication,
\end{itemize}
\end{footnotesize}
release of information be to someone without a legitimate interest in the information.\textsuperscript{28} However, it is precisely the disclosure of health information to those with a legitimate interest, such as employers, that is most problematic. The disclosure of health information to strangers often poses a marginal threat or no threat at all. Finally, to recover under an invasion of privacy theory, the plaintiff must typically establish that the disclosure was intentional, while most disclosures of health information happen by accident or through negligence.\textsuperscript{29}

Many state constitutions recognize that the right of privacy cannot be infringed without the showing of a compelling state interest. State constitutional law may come into play when a subpoena for medical records has been issued pursuant to a pending litigation, \textit{e.g.}, where medical records are sought to establish intoxication.\textsuperscript{30} The court balances policy concerns with the reasonable extent of a patient's privacy expectations. The court in \textit{King v. State}, held that medical information is such that a person would want to keep it private and thus should be entitled to any privacy protections generally provided by the U.S. and state constitutions.\textsuperscript{31} The court found that the state constitution did prevent the disclosure of medical information unless pursuant to a statute, "which effectuates a compelling state interest and is narrowly tailored to promote only that interest." In the end, the state’s statute provided more protection than the constitution,

\textsuperscript{29} \textit{See} Restatement (Second) of Torts § 652D: One who gives publicity to a matter concerning the private life of another is subject to liability 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.
\textsuperscript{30} \textit{Id.}
\textsuperscript{31} \textit{King v. State}, 272 Ga. 788, 535 S.E.2d 492 (Ga 2000).
demonstrating that filing suit under the state constitution may be futile when there are stronger state statutes in place.\textsuperscript{32}

States have varying privacy protections depending on the use and access to private information. States have specific laws that govern how open the records of the state will be, and many state agencies have agency-specific statutes governing confidentiality, access, and use of their data.\textsuperscript{33} However, little uniformity exists among state statutes and regulations protecting health information. Additionally, protections vary according to the type of information being protected, \textit{i.e.}, mental health, HIV or AIDS, substance abuse, genetic information.\textsuperscript{34} Most statutes do not address redisclosure of health information and lack penalties for misuse or misappropriation. Few states have enacted statutes and regulations as to whether medical records can be created, authenticated, and stored electronically. Only twenty-eight states explicitly protect and ensure the rights of patients to review their medical records so that they can see what information exists about them and recommend changes or make amendments if necessary. Four states allow patient access to hospital records only, whereas twenty-four provide access to both hospital and physician records.

An example illustrating the great disparity between states’ privacy laws is the enforcement of their genetic privacy laws.\textsuperscript{35} Most states have privacy laws that treat genetic information separately from other private health information, \textit{i.e.}, genetic exceptionalism. Most state privacy laws prevent certain parties from accessing or using

\begin{footnotes}
\footnote{32 \textit{Id.}}
\footnote{33 National Research Council, supra note 4.}
\footnote{34 \textit{Id.}}
\footnote{35 \textit{Id.}}
\end{footnotes}
private information in certain capacities. Thirty-six states require informed consent to disclose genetic information, other states have an additional requirement of written authorization to disclose, and several states even classify genetic information as property of the individual. This classification of genetic information is significant because it completely changes the justification for the protections. States creating this property right, however, can argue for privacy protections under the guise of property law. This problem of varying protections is not limited to genetic information but is ubiquitous throughout state privacy law.

State protection of health information is further limited by the federal Employee Retirement and Income Security Act (ERISA). This law preempts state regulation of companies that provide health care benefits through self-insurance. Due to weak federal protections, ERISA creates a considerable loophole for self-insured companies, which are not restricted from gaining access to personally identifiable health information pertaining to their employees. As a consequence, many organizations within the health care system are free to collect and use large amounts of patient-identifiable health information.

---

37 Id.
38 Id.
39 Elizabeth Hutton & Devin Barry, Privacy Year in Review: Developments in HIPAA, 1 ISJLP 347, 355 (2005). The Privacy Rule treats genetic information no differently than other private health information. HIPAA has achieved its goal of creating a “floor” of specific privacy protections in certain areas and must now expand to other areas in which disparities exist.
42 Id.
for purposes that suit their economic interests, and patients lack legal standing to bring suit against those they allege have breached their privacy.\footnote{National Research Council, supra note 4, at p. 165.}

As health care providers expand their reach across state borders, the need for greater uniformity has increased. For example, in an attempt to stimulate uniformity among states on health care information management issue, the National Conference of Commissioners on Uniform State Laws developed the Uniform Healthcare Information Act.\footnote{National Research Council, supra note 4, at p. 45; the main provisions of this model legislation are (1) to give patients the right to have access to their own medical records; (2) to allow patients to correct or amend their records if the content is suspected to be in error; (3) to require providers to obtain a written authorization before disclosing patient information to other parties; and (4) to outline situations in which patient information may be disclosed without patient authorization.} As of 2001, only two states had enacted this model legislation.\footnote{Id.} Clearly, efforts must be directed toward developing national standards of confidentiality and security to support the development of computer-based patient record systems to instill trust by consumers in the use of technology.

B. Federal Protections of Health Information

The United State’s segmented approach to privacy predating HIPAA consists of several laws. At the federal level, data protection measures are found in the Privacy Act of 1974, a few statutes that regulate narrow areas of data use, and constitutional law.\footnote{National Research Council, supra note 4, p. 37.} However, the Privacy Act sets rules only for personal data controlled by federal agencies, and other federal statutes that regulate health data processing focus on even narrower sectors of information use. Since protections for health information are subject to interpretation and have not been rigorously enforced, most health data lie entirely outside...
the protections of either constitutional or federal law, although the public policy context for protecting health information changed with the passage of the Health Insurance Portability and Accountability Act of 1996.47

The primary vehicle for privacy protections is the Privacy Act of 1974,48 which was designed to provide private citizens some control over the information collected by the federal government about them. The Privacy Act requires federal agencies to publicly disclose the existence of government record systems, allows individuals the right to access information about themselves, the right to copy, correct, or amend records kept by the government, and limits the purposes for which the federal government can collect or disclose information without consent. The biggest limitations with the act are that it only applies to record-keeping systems operated by federal agencies, it fails to provide a government oversight mechanism, the penalties prescribed under the Act are inadequate, and it mandates no specific measures for protecting privacy.49

Additional privacy protections are contained in the Freedom of Information Act of 1966 (FOIA),50 which allows individuals open access to federal agency records, except those records that are protected from disclosure by one of nine exemptions to the act. The act was created to improve public access to governmental information and promote openness in government. The disclosure of medical files, which would constitute a clearly unwarranted invasion of personal privacy, is specifically exempted from the act.

47 Id.
48 Id.
50 National Research Council, supra note 4, p. 41.
Protections under the FOIA are limited in the sense that it does not specifically prohibit disclosure of health care information held by federal agencies.\textsuperscript{51}

The Americans with Disabilities Act (ADA), which prevents public and private organizations from discriminating against individuals because of a disability, has also proven less than effective in protecting medical privacy.\textsuperscript{52} The ADA only applies to those conditions specifically defined as disabilities, and not to all health information. Another limitation of the ADA concerns its lack of practical impact: job applicants and employees are often either unaware or unable to prove that employers have made decisions based on the health information about their employees. However, the ADA may sometimes provide privacy protection by making some employers reluctant to collect and process certain kinds of personal information. Because of fear of litigation, employers may avoid collecting data regarding health conditions that place an employee or a qualified job applicant under the ADA’s protection. Collecting such data might lead to an inference of an ADA violation.\textsuperscript{53}

Two federal statutes, the United States Codes, Sections 290dd-3 and 290ee-30\textsuperscript{54} establish special rules of confidentiality for those who seek treatment for drug or alcohol abuse at federally funded facilities. These statutes apply to oral and written communication of information containing the identity, diagnosis, prognosis, or treatment of patients enrolled in treatment programs. They provide a high level of protection and allow only limited exceptions for release of patient information, including disclosure with

\textsuperscript{51} Id.
\textsuperscript{52} 42 U.S.C. §§12111-12117.
\textsuperscript{53} National Research Council, supra note 4, p. 44.
\textsuperscript{54} National Research Council, supra note 4, p. 45; 42 U.S.C. §§ 290ee-3 (1988).
the written consent of the patient. The codes protecting alcohol and drug abuse suffer from a limited scope of influence because they only apply to federally funded facilities.\textsuperscript{55}

The Medicare program has also served as a vehicle for expanding privacy protections. The Medicare Conditions of Participation requires participating hospitals to have a procedure for ensuring the confidentiality of patient records and allows information only to be released to the patient. The hospital must take precautions to ensure that unauthorized individuals do not gain access to or alter patient records.\textsuperscript{56}

Original medical records may be released by the hospital only in accordance with federal or state laws, court orders, or subpoenas.\textsuperscript{57} These conditions, however, do not address security mechanisms or evaluate practices.

An additional privacy protection can be found in the creative way one plaintiff sued for breach of privacy under Computer Fraud and Abuse Act (CFAA). The United States District Court for the District of New Hampshire held in \textit{Doe v. Dartmouth} that an unauthorized computer medical record review violates the CFAA, although the Court found that neither the language nor the purpose of the CFAA were consistent with holding the medical center vicariously liable for the doctor's intentional violation of the CFAA.\textsuperscript{58} The CFAA’s purpose is to deter and punish those who intentionally access computer files and systems without authority and cause harm. The Court additionally stated that expanding the private cause of action created by Congress to include one for vicarious liability against persons who did not act with criminal intent and cannot be said

\textsuperscript{55} \textit{Id.}
\textsuperscript{56} Medicare Conditions of Participation for Hospitals, § 482.24.
\textsuperscript{57} \textit{Id.}
to have violated the statute, would be entirely inconsistent with the plain language of the statute.\textsuperscript{59}

In the 1977 decision, \textit{Whalen v. Roe}, the Supreme Court extended substantive due process privacy protections to information privacy.\textsuperscript{60} New York passed a law requiring that records be kept of people who obtained prescriptions for addictive medications. Plaintiffs argued that the statute infringed upon their right to privacy. The court held that the constitutionally protected “zone of privacy” extends to two distinct types of interests: (1) “independence in making certain kinds of independent decisions”; and (2) “the individual interest in avoiding disclosure of personal matters.” The Court found that the statutory scheme evidenced "a proper concern with, and protection of, the individual's interest in privacy" and that the "remote possibility" of potential abuses of data accumulation and disclosure were not sufficient to establish an invasion of any rights or liberties protected by the Fourteenth Amendment. With this decision, the Court left the door open to future restrictions in light of technical change, noting that it was “not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files.” In so doing, the Court set the stage for claims that the Constitution embodies a right to informational privacy in health information, although the Court has yet to expand on this idea in any significant way.\textsuperscript{61}

\textsuperscript{59} \textit{Id.}


\textsuperscript{61} \textit{Id.}
As one court observed, the right to informational privacy “has been infrequently examined and as a result its contours remain less than clear.”\(^{62}\) The Sixth Circuit has construed the constitutional right to information privacy in a very narrow manner by only extending the right to interests that implicate a fundamental liberty interest. The court concluded that “absent a clear indication from the Supreme Court we will not construe isolated statements in *Whalen* more broadly than their context allows to recognize a general constitutional right to have disclosure of private information measured against the need for disclosure.”\(^{63}\) The right to informational privacy will be triggered only when the interest at stake relates to those personal rights that can be deemed ‘fundamental’ or ‘implicit in the concept of ordered liberty’.\(^{64}\) At least one Circuit court has expressed doubts as to whether the constitutional right to information privacy exists at all stating that the passage in *Whalen* was mere dicta.\(^{65}\) Despite the potential power of the decision set forth in *Whalen*, lower courts have failed to capitalize on this constitutional doctrine’s promise for improving health care privacy.\(^{66}\) Further, like other rights derived from the Bill of Rights, the federal constitutional right to privacy applies only against state action, requiring that the wrongful conduct be “under color of state law, custom, or usage.”\(^{67}\)

\(^{62}\) *Davis v. Bucher*, 853 F.2d 718, 720 (9\(^{th}\) Cir. 1988).
\(^{63}\) *J.P. v. DeSanti*, 653 F.2d 1080, 1090 (6\(^{th}\) Cir. 1981); see also *Bloch v. Ribar*, 156 F.3d 673, 684 (6\(^{th}\) Cir. 1988).
\(^{64}\) *Id.*
\(^{66}\) National Research Council, supra note 4, at p. 43.
C. Inadequacy of State and Federal Laws to Protect Health Information

In general, government protections of information predating HIPAA are not specific enough to cover health information. Federal and state laws attempt to balance the public’s right to access information gathered by the government and private entities against the individual’s right to protect personal information from inappropriate disclosure.68 Maintaining this balance is becoming increasingly difficult as technology provides new and improved means to collect, manage, distribute, and access data.

Before the HIPAA Privacy Rule was enacted, there were no federal standards specifically protecting the privacy and security of health information. Unless they were specifically limited by any applicable state laws, doctors and hospitals who handled personal health information could do anything they wanted with it, subject to whatever consent form the patient signed.69 A privacy law was needed to narrowly target only health information but broad enough to include within its scope all parties that maintain or transmit such information in electronic form for business reasons related to the substance of protected health information (PHI). HIPAA was the first step in better protecting health information. By mandating the promulgation of standards and regulations for security and privacy, the act began to fill the void in existing legislation for protecting health information.70

---

68 National Research Council, supra note 4, pp. 42-45.
70 National Research Council, supra note 4, p. 53.
III. INTRODUCTION TO HIPAA

During the last two decades, “safeguarding medical privacy” emerged as a key mantra in the U.S. health care debate. Despite gradual progress, until the mid-1990s, universal safeguards remained weak and the federal government left states to their own devices, resulting in nationwide discrepancies in protection levels. In 1996, the Health Insurance Portability Accountability Act (HIPAA) was passed, in part, in response to the growing concern over the privacy and security of patients' medical records and related information, in an attempt to create uniformity amongst the states.

The primary purpose of HIPAA was to “improve portability and continuity of health insurance coverage…to combat waste, fraud, and abuse in health insurance and health care delivery.” The original legislation, known as the Kennedy-Kassenbaum bill, focused on making health care insurance portable and forcing some standardization on the payor requirements. (Every insurance company or other payor had a different set of claim documentation requirements, which made it impossible for most providers to automate anything effectively). HIPAA was enacted to reduce the monetary costs of administrative operations in the health care industry and to simplify the exchange of electronic health information, with particular focus on preventing fraud and unauthorized access to, and disclosure of, individually identifiable health information. It became evident during the development of the legislation that the standardization would also

72 Id.
75 Id.
enable the compilation of a lot of very personal information across otherwise heterogeneous systems. Consequently, a set of the privacy clauses were added as protection against inappropriate use of that consolidated information.\textsuperscript{76}

Under HIPAA, Congress tasked the Department of Health Human Services (HHS) with developing federal rules and regulations that govern how patient records are handled, shared, and protected in the health care system. To accomplish this goal, Congress incorporated into HIPAA, sections 261 through 264, collectively known as the “Administrative Simplification” provisions, which empower HHS to create and publish rules to streamline the electronic exchange of health information. Additionally, in the Administrative Simplification provisions, Congress granted explicit authority for HHS to adopt rules to protect the confidentiality of individually identifiable health information.\textsuperscript{77}

Since 1996, HHS has published several sets of regulations implementing requirements that would address the security, privacy and standards for the transmittal of patient records.\textsuperscript{78}

\textbf{A. Covered Entities and Business Associates Under HIPAA}

HIPAA affects the entire medical community and their subcontractors. More specifically, HIPAA requires "covered entities," healthcare providers, health plans, and healthcare clearinghouses to implement specific measures to address the privacy of PHI and to provide specific rights to patients with respect to their PHI.\textsuperscript{79} A health care provider is one who provides health or medical services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of

\textsuperscript{76} HIPAA’s Privacy Rule, 45 C.F.R. § 164 (2005).
\textsuperscript{77} HIPAA §§ 1173, 264.
\textsuperscript{78} 45 C.F.R. § 160.310.
\textsuperscript{79} 45 C.F.R. § 160.102.
business. Health plans encompass agencies that directly provide or fund health care services. Health care clearinghouse means a public or private entity, that either (1) processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; or (2) receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity. HIPAA also places constraints on "business associates," a person or entity to whom the covered entity discloses individually identifiable health information so that the business associate can carry out or perform a function or activity for the covered entity. A business associate and a covered entity are required to enter into a written contract that imposes safeguards on the PHI used by or disclosed to a business associate.

**B. HIPAA's Three-headed Monster**

HIPAA is most often recognized today for its three main provisions promoting electronic transmission standards for claims data, and regulating both the privacy of electronic medical records and the security of medical data storage and transmission. HIPAA’s Administrative Simplification provisions are divided into three main categories known as the Transaction Rule, Security Rule and the Privacy Rule. Uniform national transaction and code set standards will save billions of dollars each year for health care businesses by lowering the costs of developing and maintaining software and reducing

---

80 45 CFR § 160.103.
81 Id.
82 Id. at §§ 164.502(e)(2), 164.504(e)(1)-(2).
the time and expense needed to handle health care transactions. Privacy and security standards assure consumers that their health information will be protected from inappropriate uses and disclosures.

In the past, the health care industry, including health care providers and insurance plans, used different electronic formats and definitions of data elements to process medical claims. As a result, data had to be reformatted and recoded before it could be shared resulting in substantially higher administrative costs. The Transaction Rule, which was the primary aim of the Administrative Simplification provision, calls for a standardized transaction and coded system that reduces handling and processing time to improve data quality and decrease administrative costs.

Transactions are activities involving the transfer of health care information for specific purposes. Under HIPAA, if a health care provider engages in one of the identified transactions, they must comply with the standard for that transaction. HIPAA requires every provider who does business electronically to use the same health care transactions, code sets, and identifiers. HIPAA has identified ten standard transactions for Electronic Data Interchange (EDI) for the transmission of health care data.

The Privacy Rule became effective on April 14, 2003, for most health care providers, health plans, and health care clearinghouses. The Privacy Rule restricts the use and disclosure of patient health information, and applies to the protection of

---

84 45 C.F.R. §§160, 162.
85 Id.
information in oral, paper, or electronic form. The rule defines a number of permitted uses, required uses, and uses for which a prior authorization is needed. It covers any record or file pertaining to the past, present, or future health of an individual, the provision of healthcare to the individual, or payment of healthcare services which contains personal identifiers such as name, phone numbers, address, medical record numbers, social security numbers, or provides a reasonable basis to believe the information can identify the individual. It addresses the use of PHI other than for treatment purposes, such as for marketing and fund raising. Further, the Privacy Rule also outlines various rights for the patient, such as the right to have access to their health information, the right to amend their health information, the right to obtain an accounting of the disclosures, and the right to request restrictions on the use of their health information. Finally, the rule places certain administrative obligations on covered entities.

Privacy and data security go hand-in-hand, and HIPAA’s Security Rule, which took effect April 20, 2005, describes what “covered entities” must do to make sure medical files are secure. The Security Rule covers health information maintained or transmitted

---

87 45 C.F.R. § 160.103.
88 Id. at §§164.502, 164.508.
90 45 C.F.R. §§ 164.514(e)-(f).
91 45 C.F.R. § 164.524.
92 45 C.F.R. § 164.528.
93 45 C.F.R. § 164.526.
94 45 C.F.R. § 164.530.
in electronic format.96 Although patients receive notice about privacy practices, data security operates behind the scenes, and like the Privacy Rule, the Security Rule is important to patients because it also creates a national standard.97 This means that all health care providers, health plans, and health care clearinghouses that transmit information electronically must adopt a data security plan.98 Section 1173(d) of the Administrative Simplification provisions empowered HHS to adopt regulations to ensure the integrity and confidentiality of electronic protected health information.99 The rule requires covered entities to take certain precautions to secure health information created, received, maintained, or transmitted by that entity and to protect against reasonably anticipated threats or hazards to the security of certain protected health information.100 Precautions include documenting formal procedures for selecting and executing security measures; implementing physical safeguards to protect computer systems and other pertinent equipment from fire, other hazards, and intrusion; processes to protect, control and monitor access to the information; and finally processes to prevent unauthorized access to the data when transmitted over communication networks or when data physically moves from one location to another using media such as magnetic tape, removable disks or CD media.101

C. Penalties Under HIPAA

Under HIPAA, the patient’s only recourse is to report the violation to the Office of Civil Rights (OCR), who may wait until complaints have accumulated before starting an

96 Id.
97 Id.
98 Id.
100 HIPAA’s Security Rule, 45 C.F.R. §§§ 160,162, and 164.
101 Id.
investigation.\textsuperscript{102} Even if the OCR performs an investigation of the procedures in place, it may or may not start the appropriate proceedings to compel compliance.\textsuperscript{103} Assuming that the OCR elects to proceed, the potential penalties are so limited that they may not serve as an incentive for covered entities to fully comply with HIPAA.\textsuperscript{104} Civil penalties are limited to one hundred dollars per incident with a cap of twenty-five thousand dollars per person per calendar year for identical violations.\textsuperscript{105} These penalties appear much too small to have the potential to serve as an incentive to ensure proper behavior. Additionally, a possible loophole may be perceived allowing entities to escape punishment, where HHS exempts violations when a failure to comply was due to reasonable cause rather than willful neglect, and the covered entity corrects the violation within thirty days of when the violation occurred.\textsuperscript{106} Covered entities can assert this as an affirmative defense shielding them from being penalized even though the breach has already occurred and an individual’s sensitive information has been leaked.\textsuperscript{107} The criminal penalties imposed under HIPAA are very limited as well, and apply only to the most egregious conduct, such as knowingly and improperly obtaining and disclosing personal information or obtaining information under false pretense.\textsuperscript{108} Only the sale or transfer of PHI for commercial advantage or personal gain is punished by a substantial prison term and fine - up to ten years in prison and a fine of up to two hundred and fifty dollars.

\begin{itemize}
  \item \textsuperscript{103} Id.
  \item \textsuperscript{104} 42 U.S.C. § 1320d-5(a)(1).
  \item \textsuperscript{105} Id.
  \item \textsuperscript{106} 42 U.S.C. § 1320d-5(b)(2).
  \item \textsuperscript{107} Id.
  \item \textsuperscript{108} 42 U.S.C. § 1320d-6(a)-(b)(2).
\end{itemize}
thousand dollars. To date, there has been only a handful of civil and criminal prosecutions.

**IV. Current HIPAA Regime**

There are many problems associated with the current HIPAA regime. HIPAA fails to address the problems of medical records security breaches and fails to provide adequate remedies, if any, to victims because there is no private cause of action under HIPAA. Another problem with the current regime is the question of enforcement. HIPAA was enacted over a decade ago and the minimum number of criminal and civil prosecutions suggest that OCR and HHS are not enforcing HIPAA. Next, HIPAA’s definition of “covered entity” is not broad enough to cover the numerous persons, many who are not healthcare workers, who might occasionally have access to a patient’s PHI. There are a number of organizations involved in the provision of care and the processing of claims who may not be “covered” under HIPAA, such as laboratories, pharmacists, or benefits managers. Although these entities may have business relationships with HIPAA covered entities, unless they are engaging in certain electronic billing and claims processing transactions, they are not covered under HIPAA. While many of these individuals have a legitimate need to see all or part of a patient’s records, no laws govern who those people are, what information they are able to see, and what they are not allowed to do with that information once they have access. A final shortcoming under the current regime is the minimal protection afforded by a business associate contract.

---

A. HIPAA Fails to Address the Problems of Medical Records Security Breaches

Numerous security breaches over the last several years have raised consumer awareness about the lack of proper security measures by most companies in protecting consumer data. As more consumer information is collected and stored in repositories for marketing and research information, many consumers are faced with the reality that their data is open to cyber criminals who are taking advantage of security holes to gain access to this information. Security breaches are very common and result in very personal information falling into the wrong hands. This scenario has been repeated many times over the last several years resulting in consumers seeking measures to secure their data. As the Internet and wireless services have matured over the years so have the threats against consumer data. As more people turn to the Internet and other wireless technologies to perform everyday tasks in the digital world, this automatically places the confidentiality of one’s lives in jeopardy. Unfortunately, for the consumer, substantial security efforts often come only after a breach has occurred.

Disclosure of PHI can occur deliberately or accidentally and can occur within an organization as a result of an external breach of security. There are several examples of recent privacy breaches that illustrate this. A Michigan-based health system accidentally posted the medical records of thousands of patients on the Internet. A Utah-based pharmaceutical benefits management firm used patient data to solicit business for its owner, a drug store. An employee of the Tampa, Florida health department took a

---

112 Id.
113 Id.
114 Furrow, supra note 1, at 337-38.
computer disk containing the names of 4,000 people who had tested positive for HIV. The health insurance claims forms of thousands of patients blew out of a truck on its way to a recycling center in East Hartford, Connecticut. A patient in a Boston-area hospital discovered that her medical record had been read by more than 200 of the hospital’s employees. A Nevada woman who purchased a used computer discovered the computer still contained the prescription records of the customers of the pharmacy that previously owned the computer. In 1993, the Boston Globe reported that Johnson and Johnson marketed a list of 5 million names and addresses of elderly incontinent women. Even companies with vigorous security programs cannot prevent some breaches, particularly those that occur from the inside.\footnote{Id.}

HIPAA’s Security Rule requires covered entities to have in place “appropriate” administrative, technical, and procedural safeguards to protect the privacy of PHI from any reasonably anticipated threats of security breaches. HHS’ flexibility of the Privacy and Security Rules means that the covered entity’s need to analyze their own requirements, then implement safeguards that are appropriate to their particular environment. HHS noted that it does not require covered entities to guarantee the safety of PHI against all “assaults.” According to HHS, the theft of PHI may or may not indicate a violation of HIPAA, depending on the circumstances of the theft and whether the entity had reasonable policies in place to protect against such theft.\footnote{Brian D. Gradle, \textit{Handling Security Breaches Under HIPAA: A Legal Perspective}, In Confidence 11:8 (Aug. 2003).}

If a security breach occurs, the covered entity has an obligation to mitigate any harmful effects that has resulted from the breach. Responses would include the
mitigation of any harm caused by the breach, the imposition of appropriate sanctions
against the members of the work force who improperly accessed or disclosed the PHI, the
training or retraining of work force members and business associates, and. The covered
entity should investigate the scope of the disclosure, including whether any information
has been disclosed outside of the entity, and to whom. Importantly, the privacy rule does
not prescribe the sanctions that must be imposed, leaving that up to the discretion of the
covered entity. If the covered entity corrects the security failure within 30 days of the
security breach, no civil penalties will be imposed by the government under HIPAA.\textsuperscript{117}

In the more than five years that have passed since the compliance deadline for the
HIPAA privacy regulations, HHS has received close to 40,000 complaints of violations,
and the majority were not eligible for enforcement. Out of those complaints where a
violation was identified, HHS resolved the cases by requiring changes in privacy
practices or other corrective actions without entering into any formal settlement
agreements or imposing any fines. Regardless of the numerous security breaches, to date,
there has only been one actual security audit of a HIPAA covered entity where the entity
was required to enter into a Resolution Agreement with HHS. Given the vast amount of
PHI available for potential breaches, HHS must take an active role by conducting more
security audits of covered entities to protect the consumer from security breaches.

B. No Private Cause of Action Under HIPAA

HIPAA does not provide for a private right of action, which is a major weakness
under the current law.\textsuperscript{118} Without a private right of action, an aggrieved patient cannot
take advantage of HIPAA to obtain redress and compensation. If a covered entity has

\textsuperscript{117} Id.
\textsuperscript{118} 45 C.F.R. § 164.500.
misused or disclosed a patient's PHI, or has not responded adequately to the patient's request to access or amend his/her PHI, the patient cannot take advantage of HIPAA to directly reach the physician, nurse, or covered entity that is responsible for the disclosure, misuse or failure to implement adequate security measures.\textsuperscript{119} Some noteworthy assistance HIPAA provides an aggrieved patient in a private right of action is the ability to sue under state law using the Privacy Rule to establish the appropriate standard of care as to what is defined as a privacy violation. In recent years, courts have allowed plaintiffs to use HIPAA standards to prove liability in privacy lawsuits alleging that their sensitive medical records were inadequately protected. For example, in \textit{Sorensen v. Barbuto}, a recent Utah case where a doctor faced an invasion of privacy lawsuit, an appeals court cited HIPAA standards in determining that the physician owed a duty of confidentiality to his patients and allowed the case to proceed.\textsuperscript{120} Also, in 2006 an appellate court in North Carolina ruled that HIPAA could be used by a plaintiff to establish the "standard of care" in a negligence lawsuit.\textsuperscript{121} These cases suggest that plaintiffs' attorneys may begin pointing to cases such as \textit{Sorensen} and \textit{Acosta} to argue that hospitals and physicians can be liable under state tort law for an "invasion of privacy" or for "negligently inflicting emotional distress" if they fail to comply with HIPAA.\textsuperscript{122}

\begin{flushleft}
\begin{footnotesize}
\begin{enumerate}
\item\textsuperscript{119}Francoise Gilbert, \textit{Global Perspectives on HIV and AIDS}, 25 Whittier L. Rev. 273, 294 (2003).
\item\textsuperscript{120}\textit{Sorensen v. Barbuto}, 143 P.3d 295 (Utah Ct. App. 2006).
\item\textsuperscript{121}\textit{Acosta v. Byrum}, 638 S.E. 2d 246 (N.C. Ct. App. 2006).
\item\textsuperscript{122}Helen Oscislawski, \textit{Courts Begin Allowing Plaintiffs to Use HIPAA as Standard in Privacy Suits}, Nat’l L.J. (June 2007).
\end{enumerate}
\end{footnotesize}
\end{flushleft}
C. Is the Office of Civil Rights Enforcing the Privacy Rule

As of July 31, 2004, the OCR initiated investigations of 7,577 complaints alleging violations of the Privacy Rule. The OCR estimates that it receives over one hundred privacy-related complaints per week, and most of the complaints involve 1) impermissible disclosure of health information, 2) absence of sufficient safeguards to prevent impermissible use of health data, 3) failure to allow patients access to their medical records, 4) violations of the minimum necessary standard for disclosure of health information, and 5) disclosure of health information without proper authorization. Over one hundred have been referred to the Department of Justice (DOJ) as possible criminal violations, yet the OCR has prosecuted only four criminal violators and imposed only one civil monetary penalty to date.

In assessing why the OCR has not imposed many civil penalties, an important consideration is the quality and legitimacy of the privacy complaints that OCR has received. To date, the OCR has rejected fifty-five percent of privacy complaints for either lack of jurisdiction or lack of a violation under the Privacy Rule even though allegations were proven to be true. Some of the complaints seem to result from a misunderstanding of the extent of protection provided by the Privacy Rule. While a large

123 Hutton, supra note 39.
124 Id.
126 Hutton, supra note 39, at 355.
127 Hutton, supra note 39, at 357.
percentage of complaints are not actionable for lack of jurisdiction or lack of violation, a number of complaints are filed maliciously. According to the January 2005 "Report on Patient Privacy," a monthly newsletter published by Atlantic Information Services, "HIPAA has become the latest vehicle of catty and even malicious patients and employees, who file meritless privacy complaints to hurt others," although the author cautions that "it's unclear how widespread the phenomenon is."

The fact that OCR’s enforcement strategy focuses more on voluntary compliance and education rather than punishment might be another consideration. In its preamble, the Privacy Rule states that the official approach to violations and enforcement is to work cooperatively with covered entities to obtain compliance voluntarily and informally before pursuing formal enforcement. The lack of civil penalties suggests that to date, most covered entities against whom there have been credible allegations of privacy violations have satisfactorily addressed the problem to prevent future infractions. While OCR has only imposed one civil monetary penalty to date, some legal experts believe that it is making a move towards more visible enforcement. Of the 13,000 complaints filed under HIPAA, HHS has successfully prosecuted only a few cases. Even though the elements of a criminal offense under HIPAA are straightforward, as to whom the provisions apply continues to be the subject of debate, and might explain why so many criminal violators are escaping punishment.

In the first criminal prosecution under HIPAA, in United States v. Gibson,

---

129 Hutton, supra note 39, at 358.
131 Hutton, supra note 39, at 356.
132 45 C.F.R. § 160.
133 Hutton, supra note 39, at 359.
phlebotomist Richard W. Gibson of SeaTac, Washington impermissibly disclosed cancer patient Eric Drew's identifiable health information to several credit card companies to obtain four credit cards in Drew's name.\textsuperscript{134} Gibson disclosed Drew's name, date of birth, and social security number, all protected health information, which had been collected by Gibson's employer, the Seattle Cancer Care Alliance, for payment of health care services. Gibson charged more than $9,000 for items including "video games, home improvement supplies, apparel, jewelry, porcelain figurines, groceries and gasoline."\textsuperscript{135} Gibson was charged with wrongful disclosure of individually identifiable health information with the intent to use the information for personal gain.\textsuperscript{136} Gibson later signed a plea agreement and was convicted and sentenced to sixteen months in prison.

Less than a year after the Gibson case, the Office of Legal Counsel of the Department of Justice (OLC) issued a Memorandum Opinion clarifying the scope of criminal enforcement under 42 U.S.C. § 1320d-6.\textsuperscript{137} The OLC Opinion specifically addressed the issue of who could be held liable for a HIPAA criminal violation and stated that only covered entities as defined under HIPAA may be directly prosecuted under the Act.\textsuperscript{138} Principles of corporate criminal liability will be used to determine the entity’s liability and the potential liability of individuals who acted on behalf of the entity.\textsuperscript{139} The

\textsuperscript{135} Id.
\textsuperscript{136} 42 U.S.C. §1320d-6(a)(3) and §1320d-6(b)(3)(1).
\textsuperscript{137} See Memorandum Opinion for The General Counsel Department of Health and Human Services and the Senior Counsel to the Deputy Attorney General on the Scope of Criminal Enforcement Under 42 U.S.C. § 1320d-6 (June 1, 2005).
\textsuperscript{138} Under 42 U.S.C. § 1320d-6, HIPAA applies only to "covered entities," such as health care plans, providers, and clearinghouses that engage in the electronic transmission of electronic data.
\textsuperscript{139} Id.
author of the OLC opinion further states that the liability of other persons who may not be directly liable under HIPAA will be determined in accordance with principles of aiding and abetting liability or of conspiracy liability.\textsuperscript{140} Whether this Opinion means that the HIPAA criminal enforcement provisions do not apply to an employee of a covered entity remains unclear and has been interpreted by some to mean that “rank and file” employees of covered entities, like Gibson, are not subject to HIPAA’s criminal sanctions.\textsuperscript{141}

The OLC Opinion tries to suppress the clear text of the criminal provision about “person”.\textsuperscript{142} The language of HIPAA states that the statute applies to a “person who knowingly and in violation of this part.” The natural reading is that “a person” can include hospital employees such as Gibson who misuse patient records, but the effect of the OLC Opinion is to change the statute to say “a person who is a covered entity who knowingly and in violation of HIPAA discloses individually identifiable information for personal gain.”\textsuperscript{143} This seems at odds with the original language of HIPAA, which includes jail time that increases based on the severity of the offense. A common sense reading of HIPAA is that Congress intended individuals who violated HIPAA to go to jail. Yet the OLC Opinion says that Congress intended to make the covered entities the target of the criminal provision, although it is nonsensical that hospitals and health insurance companies would go to jail.

\textsuperscript{140} \textit{Id.}
\textsuperscript{141} Peter P. Swire, \textit{Justice Department Opinion Undermines Protection of Medical Privacy} (Jun 7, 2005), \textltt{http://www.americanprogress.org/issues/2005/06/b743281.html}\textltt{<accessed Dec. 3, 2008>}.\textsuperscript{142} \textit{Id.}
\textsuperscript{143} \textit{Id.}
Undeterred by the OLC Opinion, federal prosecutors have pursued complaints against individual employees of covered entities. In United States v. Ramirez, defendant was indicted for knowingly using, obtaining and disclosing PHI with the intent to sell for personal gain and malicious harm. After accepting her guilty plea, the court sentenced Ramirez to serve six months in jail followed by four months of home confinement with a subsequent two-year term of supervised release and a $100 special assessment. The court found two aggravating factors that incrementally increased her punishment: the fact that defendant sold confidential medical records for personal gain and the fact that those records belonged to a federal agent.

The third and fourth HIPAA criminal prosecutions also involved the theft and sale of PHI and led to the first HIPAA criminal case to actually go to trial. In United States v. Ferrer and Machado, Machado, an employee of a medical clinic improperly obtained Medicare information and other patient information for more than 1,100 clinic patients and sold that information to the owner of a medical claims business for $5 to $10 each. Medical providers then used the stolen information to bill Medicare for services not rendered and equipment not supplied, resulting in a $7 million fraud to Medicare and approximately $2.5 million in payments to providers and suppliers. Because she testified against her codefendant, Machado’s sentence was reduced to three years of probation, including six months of home confinement, and also was ordered to pay more than $2.5

---

144 United States v. Ramirez, No. 7:05CR00708 (S.D. Tex. August 30, 2005)
145 Id.
147 United States v. Ferrer and Machado, No. 06-60261 CR-COHN, (decided by the U.S. District Court for the Southern District of Florida).
million in restitution for HIPAA violations, as well as conspiracy to defraud the
government, computer fraud, and several counts of aggravated identity theft. In 2007, a
jury in Naples, Fla., convicted Mr. Ferrer, the owner of the medical claims business, on
all eight counts as charged (one count each of conspiring to defraud the United States,
computer fraud, wrongful disclosure of individually identifiable health information, and
five counts of aggravated identity theft). Mr. Ferrer was sentenced to 87 months in
prison, three years of supervised release, and ordered to pay more than $2.5 million in
restitution.148

The fact that only four HIPAA criminal violators have been successfully
prosecuted raises concern as to whether HIPAA is actually being enforced. The barriers
created by the OLC Opinion raises the possibility that other criminal complaints may
have escaped prosecution, and might explain the DOJ’s lack of enforcement. If this is the
explanation then it would be appropriate for the OLC to reconsider its position to cover
“rank and file” employees of covered entities. Alternatively, Congress can revisit
HIPAA and amend it to apply the criminal enforcement provisions to non-covered
entities.

Recent events indicate that HHS may be moving towards more active
enforcement of HIPAA. An audit of Atlanta's Piedmont Hospital, initiated by the HHS in
March 2008, was the first of its kind since HIPAA's security rules went into effect in
April 2005. The mere fact that an audit of HIPAA security compliance was conducted

148 Id.
has many in the health care industry preparing for more unannounced audits and enforcement actions related to the data security requirements of HIPAA. 149

More recently, a stringent "resolution agreement" was signed in July 2008 by HHS and Seattle-based Providence Health & Services and is generating the same kind of buzz among health care providers that the Piedmont audit did. Providence agreed to adopt a three-year corrective action plan (CAP) and pay $100,000 to settle what HHS described as "potential violations" of HIPAA’s requirements for safeguarding electronic patient data. 150 Violations resulted from the loss or theft of laptops, optical discs, and backup tapes containing the unencrypted medical records of more than 386,000 Providence patients, when workers took the equipment out of the office. 151 Under the CAP, Providence must turn over any HIPAA-related internal policies and procedures to HHS for inspection. While Providence was audited for data security violations, many of the corrective actions it is being required to implement fall into the privacy realm, showing that HHS is making little distinction between privacy and security for compliance purposes. 152 This is the first time HHS has required a covered entity to enter into a resolution agreement. The resolution agreement with Providence indicates that the bar is being raised when it comes to HIPAA compliance and sends a clear message to

150 Id.
152 Id.
other health care providers that HHS is finally cracking down on HIPAA violators after having been accused of lax enforcement in the past.

**D. Covered Entities**

One of the major gaps in HIPAA is that there are many entities with large amount of PHI who are not in fact covered by HIPAA, and this is becoming especially noticeable in connection with the development of electronic medical records. HIPAA is not sufficient because it is not broad enough to cover all entities who have access to health information, especially the growing number who have access electronically. HIPAA covers only those who transmit health information electronically for certain administrative and financial transactions (largely related to insurance). For example, an increasing number of health care providers offer health services directly to consumers over the Internet and accept only credit card payments. These providers are beyond the scope of coverage under HIPAA.  

**E. Business Associate Contracts**

The business associate provision probably qualifies as one of the most overused and, at the same time, the most ignored portion of the HIPAA Privacy Rule. Many businesses that provide services to covered entities unnecessarily assume that the relationship constitutes a “business associate” arrangement requiring a contract. On the other hand, many covered entities and their business associates have missed the fact that a written agreement must be in place in order to satisfy HIPAA’s requirements.

---

153 Burger, supra note 69.
Examples include services for claims processing, administrative services, billing or collection services, benefit management services, researchers, or transcription services, all of which clearly involve the exchange of PHI and require a business associate contract. Business associate contracts are poorly defined and often ignored, and it is not enough to simply sign the business associate contract and place it in the file. HHS has no enforcement authority over business associates, and if they violate their contracts, HHS cannot impose civil or criminal penalties against them. Under HIPAA, business associates are only bound to the terms listed in the contract, and therefore it is the job of the covered entity to clarify the obligations and “administrative safeguards” the business associate must comply with.

Another major shortcoming of HIPAA is the fact that HIPAA’s privacy provisions do not apply to every entity with access to PHI. In its "Guidance," a set of comments and materials provided to assist in the interpretation of the HIPAA Privacy Rule, the OCR has specifically stated that a business associate contract is not required if the contracted functions or services do not involve the use or disclosure of PHI, and where any access to PHI by such person would be incidental, if at all. Vendors likely to fall within the "inadvertent disclosure" exception to HIPAA include the computer support specialist who helps install new software, who may have access to a computerized database. The plumber who comes to repair the laboratory equipment

---

156 64 Fed. Reg. 59923.
158 Id.
159 Walz, supra note 155, at 520.
might find files with test results near the sink. Sales representatives or a service provider may pass by a desk and be able to read PHI displayed on computer screens or handwritten notes.

The OCR specifically carves out janitorial services as an example of subcontractors that would not need to be bound by a business associate contract. This is of great concern because janitors have daily access, outside of regular office hours and with minimal supervision to premises where healthcare is provided and patients are treated. Janitors frequently have permission to open more doors and access more offices than physicians who are bound by the Hippocratic oath and risk losing their medical license in case of wrongdoing. It is troublesome that OCR made it a point to exempt from the Privacy Rule persons who are responsible for emptying wastebaskets that may contain notes or duplicates of personal records with sensitive PHI. Private investigators and others know very well that excellent reliable, up-to-date information can be found in a company's garbage.

V. Movement Towards Health Information Technology

Increasingly sophisticated technology presents opportunities in advancing integrated healthcare, improving access and quality of care, and reducing administrative costs. With electronic medical records stored on a centralized platform, there is the potential for fully integrating systems and applications that will move the nation’s healthcare system into the twenty-first century. Doctors will have the ability to quickly access a patient’s entire medical history to accurately diagnose and treat, while the

160 Id.
161 Id.
162 Id.
163 Id.
computer will help reduce human error and adverse events by flagging errors. Insurers and payers will see huge cost savings with the ease and access a centralized system will bring. Society and consumers will realize the most benefits because of an increase in their quality of care. The opportunity to modernize health care exists but the lack of uniform regulation may inhibit the adoption of Health Information Technology (HIT). The movement towards HIT will strongly be facilitated by the industry’s use of electronic health records and the formation of large clinical data repositories for health services research and medical outcome studies.

A. Industry’s Adoption of Electronic Health Records (EHR)

Efforts are needed to help move health providers to “paperless” electronic medical transactions, which will allow information to be exchanged more efficiently and should result in better service for consumers.\textsuperscript{164} Electronic records will be more complete, more legible, and more accessible to providers. The issue of electronic medical record confidentiality is a double-edged sword. Patients want their medical history secure and known only to their healthcare provider. Unfortunately, payers, regulatory agencies, service organizations, researchers, marketers, and other third parties are accessing healthcare information. Medical records are generally viewed by more individuals and organizations than any other private, personal record.\textsuperscript{165} Electronic health records offer improved efficiency in accessing medical records at a presumably


\textsuperscript{165} \textit{Id.}
lower cost and would overcome serious and frequent problems regarding the availability of paper-based medical records.\textsuperscript{166}

While there have been well-publicized breaches in the security of paper-based medical records, their inherent limitation is also a safeguard (\textit{i.e.}, the sheer size and volume of any paper medical record inhibits massive theft). Conversely, EHRs in a computerized patient database can be easily copied or changed without the appropriate safeguards. The threat of easy access to electronic medical information was recently highlighted by an incident at a hospital in Michigan. A university student was able to access, through the hospital’s public web site, private medical data normally used for scheduling (\textit{i.e.} patient names, addresses, phone numbers, social security numbers, employment status, treatments for specific medical conditions, and other data).\textsuperscript{167} This incident highlights the need for properly maintained security procedures, such as a simple password protection and encryption for patient data.\textsuperscript{168}

\textbf{B. Introduction to EHR Data Repositories}

An EHR conceived as a stand-alone file on a USB stick would appear to be a safe way to ensure the individual’s privacy, yet lacks any protections if it falls into the wrong hands. However, almost no one with ambitions for EHRs and HIT wants to leave them at this level.\textsuperscript{169} The ultimate goal of the EHR is to make all patient information immediately accessible and easily transferable and to allow its essential elements to be

\begin{flushleft}
\textsuperscript{166} Id at p. 9.  \\
\textsuperscript{167} Id.  \\
\textsuperscript{168} Id.  \\
\end{flushleft}
held by both physician and patient.\textsuperscript{170} Ensuring the integrity and availability of EHR data whenever and wherever a patient may need access to it requires both backup copies and a communications platform to reach those backups, which led to the emergence of players providing “repository” services.\textsuperscript{171} Online repositories will allow patients to store, retrieve, manage, and share their health data such as lists of medical problems, medical history, medications, allergies, test results, insurance information, and doctor’s visits over the Internet. Robust functionality for EHRs requires the ability to exchange their data with the parties that provide health services to the patient – \textit{i.e.}, physicians in clinics, hospitals, and pharmacies. Although their functionality is currently limited, some online data repositories feature the capacity to “catalog existing health records, receive test results, or monitor current physical readings.”\textsuperscript{172}

One of the first online health data repositories was Dossia, which was founded by AT&T, Intel, Wal-Mart, and five other large U.S. employers, and offers a voluntary means of storing personally controlled health data to about 2 million employees and 5 million dependents and retirees. Dossia’s long-term goal is a portable and secure lifelong health record that will be available regardless of a person’s employer, insurance plan, or physician, and employees who leave a participating organization will still be able to use the system.

Microsoft HealthVault is another service that will allow patients to collect, store and share health information with family members and participating healthcare providers. HealthVault is currently only available in the United States and includes a search feature,

\textsuperscript{171} Cushman, supra note 169.  
\textsuperscript{172} Id.
services (such as an emergency health record) to which information can be sent, and a connection center permitting the direct upload of data from compatible devices, such as those that measure heart rate, blood pressure, blood glucose, or peak airway flow. Microsoft indicates that it does not “use your health information for commercial purposes unless we ask and you clearly tell us we may.”\textsuperscript{173}

Google Inc. will be one of the first Internet service providers to begin storing medical records. Each health profile, including information about prescriptions, allergies and medical histories, will be password protected similar to other Google services such as e-mail and personalized search tools. Google’s pilot program launched in February of 2008 with the Cleveland Clinic and enrolled approximately 10,000 patients to test the platform’s ability to exchange data with an electronic medical records system. Such exchanges could eventually allow patients to store all their medical records in one place and to communicate with providers, pharmacies, and online health applications.\textsuperscript{174} Google views its expansion into health records management as a logical extension because its search engine already processes millions of requests from people trying to find more information about an injury, illness or recommended treatment.

Online repositories promise consumers “complete control over their data,” meaning that personal information will not be sold or shared without the consumer’s explicit permission. Repositories may have comprehensive privacy policies, and people can always delete their data or cancel their accounts. Unfortunately, promises about data privacy and security may lack legal force. Policies about advertising on repository sites

\textsuperscript{174} \textit{Id.}
vary from complete prohibitions to allowances for targeting ads and searches to users with specified personal characteristics. The potential advantages of EHRs stored in online data repositories are tremendous, however, their current limitations and potential downsides must be considered before blindly accepting EHRs.

C. Advantages of Online EHRs

The societal advantages of EHRs stored in centralized repositories with a fully integrated health care system are tremendous. Patients do not have to pay for online storage or other costs of maintaining online health data. Funding for online repositories are largely based on anticipated revenues, and patients will not have to pay for online storage or other costs of maintaining online health data. The majority of revenues for providers such as Google and Microsoft will come from the inclusion of search engines that allow consumers to conveniently investigate health-related topics and generate lucrative advertising opportunities. Revenues for hospitals and health plans will come from the recruitment and retention of patients who want such records. Additionally, the anticipated savings for insurers come in the form of reductions in claims as a result of coordinating care and enrolling patients in disease-management programs. Benefits for employers will come in the form of increased worker productivity and decreased health care costs for employees who become more aware of their health care needs. Employees will be able to utilize the providers’ wellness programs more fully and have better-coordinated care. The federal government, who is the largest payer of health care costs, will realize the greatest benefit of the industry’s adoption of EHRs. The government will

---

175 Id.
176 Hartzband, supra note 170.
177 Steinbrook, supra note 173.
see a decrease in health care spending as EHRs eliminate superfluous expenses resulting from medical errors or unnecessary testing and the improved quality of care will decrease health care expenditures in the long-run.

Storing EHRs online in data repositories has several advantages to the patient and provider over the traditional paper based medical record. A patient’s history, physical exam findings, medications, lab results, and all physicians’ opinions will be collected in one place and be available at a single keystroke. Users of online repositories can access their accounts from any Internet-connected personal computer, control what information goes into the profile, and regulate who is permitted to see it. In theory, personally controlled online health data could help improve health, doctor-patient communications, and the coordination and quality of care, and avert medical errors resulting in a reduction of the cost of care. The users who would benefit the most may be patients with complicated chronic conditions and those with episodic needs for extensive care or treatment.\(^{178}\) Updating, sorting, and searching through EHRs will be much easier than looking through a folder full of physician notes, lab results, and x-rays to find the one piece of information that is needed. However, the state of a fully integrated system is still in its infancy, and the real benefits are yet to be seen.

**D. Disadvantages of Online Medical Records**

Health information technology is one step towards utilizing better tools to identify errors and measure safety trends. The expansion of health information technology and personally controlled electronic health data raises a host of new problems and exacerbates old ones. Unfamiliarity with technology, especially when an EHR program is first implemented.

implemented, can significantly detract from patient time as the doctor or nurse struggles with unfamiliar equipment. Many patients report instances where the doctor has to divert focus to figure out how to enter things electronically leaving less time for the patient. Along with reduction in doctor/patient time, some people find that electronic medical records and their accompanying systems have depersonalized doctor visits or communications with a doctor’s office. For instance, protocol of a system may require any patient’s questions to be emailed to a doctor rather than communicating them by phone, which can increase wait time for replies, especially if emails are not checked regularly. Reliance on EHRs will place the health care industry at the mercy of technology, and computer glitches or Internet failure could severely hinder medical care. The nature of human error also makes it easy to miss recording relevant details, or to type in incorrect information when working with new technologies.

Consumers or their service provider are faced with a few options for getting paper records into an online health data repository, either faxing or scanning the documents into an electronic file, manually re-keying the information in, or using the repositories applications to upload EHRs. Repositories allow consumers the ability to modify their information in the repository. According to their policies, users have the ability to delete any of their information stored in the repositories. Users can edit any information they have entered in their account at any time, and their account will reflect their changes immediately. Users can also add notes to the information sent to their account by a health care provider. The entire integrity of the health care system is at risk if patients have the ability to modify their health information, which will allow them the opportunity

---

179 Hartzband, supra note 170.
to engage in fraudulent behavior. Manipulation of data might alter the EHRs such that they will not accurately reflect a consumer’s current health condition. In turn, a physician who may rely upon the EHRs may not be able to fully diagnose and treat the patient, leading to increases in medical errors. The data may be incomplete, inaccurate, or difficult to verify, resulting in liability concerns for physicians who rely more heavily on EHRs as the HIT movement progresses. Consumer access must be limited in order for these repositories to reach their full potential.¹⁸⁰

Along with advances in technology come increased threats in terms of privacy and confidentiality of medical information. Although the electronic exchange of health information has the potential to improve the quality of health care, the privacy risks of a computer-based information system are numerous. Computerization of medical records make large amounts of detailed personal data more readily accessible and transferable not only to health care providers but to others. When a breach in confidentiality occurs, it is often with respect to hundreds if not thousands of records at a time.¹⁸¹

Perhaps the most significant disadvantage of online medical records is that online data repositories such as Dossia, Google Health, and Microsoft HealthVault are not covered entities subject to HIPAA, so the data they store may not be as private as consumers assume and a person’s control over their information could be very limited. Privacy concerns stem from watchdogs who believe Google and Microsoft already know too much about the interests and habits of its uses as its computers log their search

¹⁸⁰ Google Health’s privacy policies state that “users can delete any of their health information stored on Google Health and edit any information they have entered in their account at any time, and their account will reflect their changes immediately. They can also add notes to the information sent to their account by a health care provider.” ¹⁸¹ Joy Pritts, Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule, Yale J. of Health Policy, Law, and Ethics (Spring 2002).
requests and store their e-mail discussions. A patient who agrees to transfer medical
records to an external health service run by Google or Microsoft could make it easier for
others to obtain the information. Google runs the Internet’s most lucrative ad network,
basing its marketing messages on search requests and the content on Web pages and e-
mail contained in its computers networks. Google’s recent purchase of DoubleClick, the
largest database collection agency for target advertising, provides Google the leading
platform in Internet advertising. Without the marketing protections under HIPAA, there
is nothing preventing DoubleClick from accessing an individual’s health information
placed on Google Health for target advertising purposes.

VI. ONLINE DATA REPOSITORIES AND HIPAA

Providers such as Microsoft and Google are not legally required to comply with
HIPAA because the text of the law only includes medical practices, hospitals, labs, and
insurance companies, but has no provision for any additional providers. Microsoft
HealthVault and Google Health clearly state that they are not covered entities or business
associates as defined by HIPAA. If an individual or physician signs up for Microsoft or
Google’s repositories, the legal protections afforded by HIPAA no longer apply. Online
data repositories have privacy policies in place for the protection of data, but in case of a
breach or loss of data, an individual’s only recourse is under the general privacy laws,
and that recourse may be limited because he/she voluntarily placed the information
online. Additionally, these services are not legally prohibited from disclosing an
individual’s health information to third parties for marketing. Finally, the lack of
procedural subpoena protections is another disadvantage of not being protected under HIPAA.\(^\text{182}\)

**A. Online Repositories Are Not Covered Entities or Business Associates Under HIPAA**

Providers such as Microsoft and Google are not legally required to comply with HIPAA because they are not covered entities as they are neither a health services provider nor a payer. The applicability of HIPAA's privacy protections depends on the entity that processes the healthcare record, so unless the EHR vendor is itself a covered entity under HIPAA, the Privacy Rule does not apply. The basic idea is that if a healthcare provider (hospital, physician, pharmacist) or a health plan maintains an electronic health record, that record is protected under HIPAA. As the Department of Health and Human Services noted, unfortunately, this leaves many of the people and organizations that receive, use and disclose protected health information outside of the system of federal protection.\(^\text{183}\)

Online data repositories are not required to sign a business associate contract under HIPAA because their primary relationship exists with the consumer themselves and not the covered entities. The data repositories state they do not provide business associate functions under HIPAA because they are only used by patients to manage their own information and not by HIPAA covered entities to manage medical records. These providers say they are not an electronic medical records system or a service to HIPAA covered entities, which would eliminate the need for a business associate contract.


However, applications will exist for HIPAA covered entities to populate their own systems with information from these data repositories. These applications will also allow covered entities to transfer data to their patients who are data repository users. Since some or all legal protections for consumers may be lost when data is transferred from providers to a non-covered entity, it seems even more important to have at least a business associate contract in place before transferring data into online health repositories.

**B. Online Repositories Have Their Own Privacy Policies**

Migration from physical to electronic media greatly enhances security and privacy issues. The World Privacy Forum warned recently of the importance of understanding the privacy risks that exist before sensitive medical information is shared outside the healthcare sector, since privacy protections do not generally follow a health record. HealthVault and other online medical record repositories reside outside of the protections of HIPAA.\(^{184}\) These repositories have their own privacy policies in place and are based on corporate policies developed over years with attention to privacy issues, influenced by input from privacy and health advocates.\(^ {185}\) However, these policies were developed by for-profit entities to protect its own commercial interest, and it cannot be ensured that the consumers’ personal interests are the focus of the policies.

Data repositories only share one’s personal health information with third parties, such as health care providers, when the individual authorizes consent to share. The

\(^{184}\) Page, supra note 182.

repositories contain a directory of third-party websites, which may include one’s medical provider, who are capable of securely sending and receiving health information. Repositories will allow the individual to extend access to these third parties by permitting them to send information such as medical records, prescription histories, or test reports. Once the individual agrees to share their information with a third party, he/she can view a list of those who were granted access and can revoke sharing privileges at any time. Although access has been revoked and that party will no longer be able to read the individual’s information, the third party may have already seen or retained a copy of the information.

The published policies of Google Health highlight the lack of protection for consumers who grant third-party access to their PHI. Google appears to be relinquishing any liability once the individual’s health information is in the hands of the third-party. Although third-party websites listed in the directory are contractually required to abide by the data repository policies, which establish “strict” privacy standards for how they collect, use, or share health information, the repository’s privacy policies state that they are not responsible for the content, performance, or privacy policies of third-party websites. Once access has been granted to a third-party, that party’s privacy policy will govern who will access and use the PHI, and others at that facility, such as doctors, nurses or administrative staff will be able to view PHI.

Although some of these third-party websites will be covered under federal and state health privacy laws such as HIPAA, it will be virtually impossible for the average

consumer to determine what protections govern each third-party website they grant access to.

C. Marketing PHI To Third Parties

The marketing prohibition of HIPAA does not apply to EHRs that are maintained outside of covered entities. The main privacy concern is that the records residing outside the healthcare system are at the very least open to commercial exploitation and private health information will leak into marketing systems. While physicians may be bound by privilege and medical ethics not to exploit or divulge patient records for personal gain, commercial repositories do not operate under the same legal and ethical constraints. A 2007 study of record repository privacy policies conducted for the Department of Health and Human Services found that only one in thirty repository privacy policies stated that explicit consumer consent was necessary prior to the sharing of any personal health data by the vendor. Microsoft and others maintain that the design of their repositories provides more, not less, protection than HIPAA, but those assurances do not assuage privacy advocates' concerns. It is possible, perhaps even likely, that by sharing health records with a third-party repository, consumers will be seen to have waived any privilege that previously applied to their medical records. The terms under which a record repository operates could allow the sale or rental of consumer information in the same way that magazines, catalog companies, charities, or other merchants share information with little if any consumer knowledge or consent.  

187 Page, supra note 182.
D. Non-HIPAA Entities Lack Procedural Subpoena Protections

Records in a non-HIPAA covered repository also lack the basic procedural subpoena protection provided by HIPAA. Under HIPAA, if someone wants to subpoena a consumer’s health records from a covered entity, the entity seeking the records must first notify the consumer. With that notice, the consumer has the chance to contest the subpoena, argue that the request is too broad, object that the records are not relevant, or seek a protective order. Protections covering subpoenas of health records provided by HIPAA will not apply to personal health records housed in a third-party repository.188

VII. POTENTIAL SOLUTIONS SO HIPAA DOES NOT BECOME OBSOLETE IN INDUSTRY’S MOVEMENT TOWARDS HIT

HIPAA’s major flaw is obsolescence because it is based on the wrong technology model: an early-1990s world in which electronic health information was stored in payer and provider legacy systems, proprietary applications incapable of integrating with the modern HIT movement. The industry’s movement towards HIT and EHRs has outpaced HIPAA, which pre-dates the Internet explosion and broadband connectivity. Now providers and payers store huge fields of data in a common cyberspace accessible with any Internet connection.189

It is apparent to any common observer that there has been a rapid explosion in the use of the Internet by organizations and individuals. The universality of the Internet simplifies communication, sharing of data, and transactions. The Internet offers tremendous potential for provider-to-provider communication (i.e., physician-to-hospital, physician-to-pharmacy) and consumer-to-healthcare provider communication. Access to

188 Id.
healthcare information in rural and underserved areas has improved through the use of telemedicine. It is now common for consumers to access health-related web sites for health information or enter chat rooms with individuals in health related support groups and health experts to discuss medical issues.\textsuperscript{190}

Members of the medical and IT industries claim that medical and health data must flow freely if advances in research and development, and treatment, are to be realized. Consumers want the benefits of HIT enabled healthcare, yet they want the assurances that their information will be protected.\textsuperscript{191} The risks of inadequate computer and Internet security include harm to a patient, liability for leaked information, loss of reputation and market share, and promotion of public mistrust of the technology. Problem areas include the ease in compromising security of password-protected access sites, which can result in interception of private data and allow hackers to easily impersonate the intended user. Additionally, data integrity and cyber terrorism are real threats as are the tremendous propagation of new and debilitating computer viruses.\textsuperscript{192}

Consumers would be more willing to place their health information into data repositories knowing there is a federal law in place to protect their PHI. The California HealthCare Foundation received prominent play in national media with a detailed report on the large gaps between the declared privacy policies of major Internet health sites and the actual vulnerability of website visitors to third-party collection of their intimate, individually identifiable health-related information. Noting the limitations of covered entities in the Privacy Rule, the report came to the conclusion: “Many of the new e-

\textsuperscript{190} Bogen, supra note 164, at p 13.
\textsuperscript{191} Burger, supra note 69.
\textsuperscript{192} \textit{Id.} at 13.
health companies and services now proliferating on the Web are outside this definition, yet they collect and store vast amounts of personal health information.\textsuperscript{193}

For all its shortcomings, HIPAA was the catalyst that started the HIT movement in this country, and without HIPAA the push for EHRs would not have been so strong. It opened the doors for a new relationship between providers and payers to transact information more easily and freely. Current weaknesses may inhibit the nation’s movement towards HIT while limiting the interests of consumers, and for HIPAA to have the effect Congress intended it must be expanded to cover more entities that have access to one’s health information. At the least, HHS should require data repositories to sign business associate agreements to protect consumers until Congress can act

\textbf{A. Congress Must Revisit HIPAA and Revise Definition of Covered Entities}

There is no question that a privacy law specifically protecting health information is needed, and HIPAA is adequate in this regard. There was an obvious need for comprehensive federal legislation when HIPAA was first enacted, but the Privacy Rule is limited in scope because it does not cover all entities with access to PHI.\textsuperscript{194} The advances in HIT are quickly outpacing the protections afforded to PHI, and Congress must revisit HIPAA and build upon the existing protections to protect PHI in the modern electronic environment. "For one thing, HIPAA is a statute and has the force of law," said Pam Dixon, executive director of World Privacy Forum. "If health records are stored outside of HIPAA protection, then consumers must rely on repository privacy

\textsuperscript{194} Cunningham, supra note 193.
policies. Those policies can be changed at the whim of the company and can be made retroactive and consumers would have no legal recourse.\textsuperscript{195} One out of many examples is when Gateway Learning Corporation collected personal information from its consumers, and its privacy policy stated that it would not sell, rent, or loan personal information to third parties unless people consented. Subsequently, Gateway altered its privacy policy to allow the renting of personal information to third parties without informing customers or obtaining their consent.\textsuperscript{196} The healthcare sector is in a transitional phase and society must make a decision as to whether healthcare records should be protected by the medical sector where they have always been, or should they be outside where access may be more convenient but protections are less certain.\textsuperscript{197} "The problem is, once those records are outside the healthcare sector, the marketing prohibition lifts, and those records can make their way into the wrong hands, such as employers or insurers," Dixon said.\textsuperscript{198}

HIPAA could be broadly interpreted as covering online health repositories. Under HIPAA’s provisions, any information that is, or reasonably could be, linked to an individual is PHI, which is defined very broadly as anything related to the “past, present or future physical or mental health condition” of a person.\textsuperscript{199} Additionally, HIPAA’s Privacy Rule applies to PHI in “any form or medium” which includes paper records as well as electronic ones, faxes, emails, exchanges in phone conversations, and even talking face-to-face. If the information is health data and is identifiable, then it is

\begin{footnotesize}
\textsuperscript{195} Page, supra note 182.
\textsuperscript{196} In re Gateway Learning Corp., No. C-4120 (Sept. 10, 2004).
\textsuperscript{197} Page, supra note 182.
\textsuperscript{198} Id.
\textsuperscript{199} 42 U.S.C. 1320d4-b.
\end{footnotesize}
“covered” and therefore, information stored in Google’s or Microsoft’s data repositories should be covered under HIPAA. However, the current definition of a covered entity allows online data repositories such as Google and Microsoft to escape the obligations under HIPAA.

Congress must clearly define that any repository facilitating the exchange of PHI will be considered a covered entity under HIPAA. The Workgroup for Electronic Data Interchange, a large constellation of insurers, providers, government agencies, and vendors that was established during the Bush Administration, is among those arguing for the scope of the rule to be expanded, suggesting that all entities involved in electronic exchange of individually identifiable health information should be included in the rule as health care clearinghouses, which are covered entities under HIPAA. Congress must legislate through a one-size-fits-all approach by expanding the scope of the definition of a health care clearinghouse to all entities involved in the electronic exchange of PHI. This action would vest the authority for HHS to issue regulations setting standards to regulate the electronic exchange of PHI through data repositories. If EHRs stored in health repositories were given equal privacy protections to institutional records of covered entities, they could come to be the preferred venue for PHI.

The environment is rapidly evolving, and regulations that are tailored to particular roles and contexts will be needed in order to best protect consumers and allow sufficient room for innovation. Some of the protections may be best implemented through the industry’s best practices with oversight from HHS. HHS must come up with

Cushman, supra note 173.
Cushman, supra note 173.
recommendations for privacy and security protections for EHRs, particularly when handled by entities that are not part of the health care system. Standards must be established for notification in the event of a breach, and HHS should be required to report annually to Congress on enforcement of the HIPAA Privacy Rule. HHS must be careful to use a scalpel, and not a hatchet, when issuing regulations to ensure they do not stifle further innovations in the HIT movement.

B. Until HIPAA is Revised, Data Repositories Should Sign a Business Associate Contract as a Minimum Safeguard

As a stop-gap measure before Congress attempts to revisit HIPAA and revise the definition of covered entity to cover online data repositories, such as Google and Microsoft, HHS should protect consumers by requiring online data repositories to sign a business associate contract at the least. If a repository service like Google Health or Microsoft Health Vault is facilitating in the exchange of information between providers, patients, and payors, they clearly have access to PHI. Although the repositories interpret their relationship between themselves and the consumer, HHS must challenge this interpretation. The data repository can be interpreted as functioning as an entity acting on behalf of a covered entity so one response would be for the covered entity to secure a business associate contract before transferring information to it. Signing a business associate contract will at least place minimum safeguards that are enforceable under contract principles in case of a breach. Alternatively, HHS could require covered entities to request the patient’s specific authorization for single or on-going transfers to any repository.
C. OCR’s New Guidance on HIPAA’s Privacy Rule and the Electronic Exchange of Health Information

Recently, the OCR published a new set of guidelines regarding the electronic exchange of health information in a networked environment. HHS is using HIPAA’s Privacy Rule as a foundation for when HIPAA covered entities participate in the electronic exchange of information by disclosing PHI to a separate legal entity called a health information organization (HIO). An HIO is defined as an organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards. The new guidelines place similar HIPAA constraints on HIOs to those faced by the traditional covered entity, and even though HIOs are not considered covered entities, they will be required to sign business associate contracts because they facilitate the exchange of PHI for treatment, payment, or operations. As the health care industry shifts into the electronic age, the new guidance demonstrates that HHS has recognized the risk associated with the various entities participating in the electronic exchange of health information. Although the new guidelines only provide guidance to HIPAA covered entities and business associates participating in the electronic exchange of health information in a networked environment, the OCR’s recent action is one step towards expanding HIPAA to cover other entities offering EHRs online.

204 Id.
205 Id.
VIII. CONCLUSION

Consumers and health care providers want not only the benefits that health information technology is able to provide, but also, the assurances that their PHI will be protected. Systems can be developed that provide suitable protections against unwarranted uses of health information while respecting the need for legitimate access. Individuals should be able to interact in modern society without losing control over their personal information. The modern right to privacy also entails the right to control our personal information even after we disclose it to others. HIPAA’s Privacy and Security Rules were Congress’ attempt to restore the public’s confidence regarding sensitive medical information strictly as a matter between a patient and his/her doctor. Even after the passage of HIPAA, many patients believe their health information is not protected for several reasons: the number of organizations involved in the provision of care and the processing of claims, increased efforts to market health care and other products to consumers, and the growing use of electronic information technology. One out of five adults believes that healthcare providers, insurance plans, government agencies and employers have improperly disclosed personal information.

Gaps in federal privacy protection coverage under HIPAA leave large volumes of identifiable health information vulnerable to improper access and disclosure without any real remedies. The rapid growth of the electronic exchange of health information heightens the urgency of filling these gaps through federal legislation. Forming a

---

206 Link, supra note 111.
207 Furrow, supra note 1, at 333.
national health information infrastructure without adequate federal privacy protections threatens not only the privacy of patients but also the very viability of such a system. HIPAA itself can hardly be blamed for the lack of cogent federal policy on e-health. The world has changed too rapidly, and a partisan government moves too slowly to keep up. The challenge moving forward, as a new Congress and new administration begin their work, will be to fashion coherent and constructive federal policies that enhance the use of new information technologies in health across a confusing jumble of competing viewpoints, interests, agency turf, and committee jurisdictions.\textsuperscript{209}

HIPAA, the cornerstone of federal policy on information technology in health care, was an ambitious law that was conceived just before network computing and the World Wide Web revealed themselves as the building blocks of a new electronic marketplace. As a result, federal policy makers remain locked in a framework that does not properly fit the challenges the emerging electronic marketplace pose for the health system. There was huge pressure on Congress not to write rules on e-commerce that would stifle innovation, but lawmakers risked undermining consumers’ confidence in the virtual marketplace when they left advertisers and information brokers free to exploit the gold mine of data stored on health information data repositories.

History has demonstrated that the current health privacy laws are inadequate to protect health information stored in online repositories. Instead of implementing new laws filling in the gaps HIPAA leaves open, Congress must revisit the existing health privacy law and expand the scope of coverage under HIPAA. Not only would this ease consumer fears in the movement towards electronic health records, but also, expansive

\textsuperscript{209} Cunningham, supra note 193.
legislation would encourage more to go electronic. HIPAA must catch up with the movements in health information technology by expanding coverage to repositories containing one’s personal health information. Until Congress amends HIPAA to cover all entities with access to PHI, HHS should require data repositories to sign business associate contracts.