1-1-2011

Electronic Medical Records and the Challenge to Privacy: How the United States and Canada are Responding

Elana Rivkin-Haas

Follow this and additional works at: https://repository.uchastings.edu/hastings_international_comparative_law_review

Part of the Comparative and Foreign Law Commons, and the International Law Commons

Recommended Citation

Available at: https://repository.uchastings.edu/hastings_international_comparative_law_review/vol34/iss1/6

This Note is brought to you for free and open access by the Law Journals at UC Hastings Scholarship Repository. It has been accepted for inclusion in Hastings International and Comparative Law Review by an authorized editor of UC Hastings Scholarship Repository. For more information, please contact wangangela@uchastings.edu.
Electronic Medical Records and the Challenge to Privacy: How the United States and Canada Are Responding

By ELANA RIVKIN-HAAS

I. Introduction

Once a simple interaction based on trust, the doctor-patient relationship has been dramatically reshaped by the modern health care system. Treatment has become specialized, often spread among numerous healthcare providers, requiring that patient records be available to be viewed by many. Moreover, technological advances have made comprehensive electronic health record storage a viable reality, forcing consideration of new legal and ethical questions regarding privacy.

A centralized electronic medical records system seems attractive for several reasons: It has the potential to facilitate increased communication between healthcare providers and patients, to help decrease costs, and to improve the overall quality of care. However, for electronic health records to be successful, patients must feel confident that their personal information will be secure; otherwise, they may be unwilling to disclose critical information. This unwillingness would prove detrimental to the quality of their healthcare and thus to their health. Currently, a tension exists between the push toward electronic centralization of medical records

---

and the need to protect patients' private information.

Electronic medical records allow for increased availability, aggregation, and dissemination of medical information. With the spread and advances of technology, the number of people who potentially have access to an individual's sensitive health information increases dramatically. This ease of information flow, in some ways, conflicts with notions of patient decisional autonomy. Patients may consent to having their health record stored in a centralized, electronic system, but exactly how patients' expectations and beliefs about how that information will or should be used, and who will or should be able to view it may vary widely. Thus, in many cases, access and secondary uses of personal information may exceed the scope of what patients, upon disclosure, believe they have consented to. The privacy concerns in the technology era, therefore, stem primarily from insufficient control by patients over secondary uses of health information and the future harms that may result from such unauthorized or undesired access to such information.

This paper first examines the existing privacy law standards applicable to medical records in the United States and Canada and then considers whether the current privacy framework offers patients adequate protection against these new privacy concerns. Section II will consider the common law of privacy and how, if at all, it can apply in the context of electronic medical records. Section III will focus on constitutional interpretations of privacy in both the U.S. and Canada. Section IV concludes the piece with a comparison of the statutory schemes currently governing electronic health records in the U.S. and Canada.

II. American Common Law

"Privacy" in both American and Canadian societies means many different things to different people, reflecting the complexity of the term and the wide range of ways the concept is employed in these legal systems. As one scholar explained, "[t]he term 'privacy' is an umbrella term, referring to a wide and disparate group of related things." Because the term "privacy" is used so broadly, it can often be difficult to tell exactly what it means to "violate" one's privacy. At a basic level, the concept of privacy connotes that some information, some decisions, and our physical body should be free from intrusions.

by others. As Justice Brandeis and his co-author Samuel D. Warren wrote: "the right to life means the right to enjoy life – the right to be let alone."³

Physical invasions of one’s person without consent form the basis of the traditional torts of battery and assault and usually present a clear kind of injury from unwanted physical contact.⁴ Brandeis and Warren, however, talked about invasions of privacy that caused no direct, physical injury. Instead, they focused on invasions of privacy that involve injury to feelings.⁵ They recognized that incorporeal harm resulting from damage to one’s “reputation” through defamation, etc., could be legally cognizable.⁶ Thus, a right to privacy, in some ways, means the right to protect one’s personal dignity.

Prosser expanded upon the ideas of Brandeis and Warren, synthesizing redressable privacy violations as

1. intrusion upon the plaintiff’s seclusion or solitude, or into his private affairs;
2. public disclosure of embarrassing private facts about the plaintiff;
3. publicity which places the plaintiff in a false light in the public eye;
4. appropriation, for the defendant’s advantage, of the plaintiff’s name or likeness.⁷

However, these traditional American torts that result in an invasion of privacy offer remedies for only a narrow range of circumstances in the healthcare context. Only the torts of intrusion and public disclosure appear applicable, and even these have certain limitations.⁸

For example, to bring a successful suit for public disclosure, the

---

4. Solove, supra note 2, at 487.
5. Warren & Brandeis, supra note 3, at 197.
6. Id.
information disclosed must be of a shameful nature. This confines
the protection offered by this tort to health information that is of an
"unpleasant or disgraceful" nature or pertains to an embarrassing
disease or some "hidden physical or psychiatric problems." It would
seem, then, that much of a patient’s health information may not be
protected because it does not fit the “shameful” criteria. Further,
"the success of a privacy tort claim hinges on an assessment of the
reasonableness of the victim’s expectation of privacy in the space
invaded or information disclosed," and “[a]s a general rule, if
information has been voluntarily disclosed by a patient to anyone in a
non-fiduciary capacity . . . it is no longer deemed ‘private’ and
therefore privacy torts do not apply.” Thus, none of these violations
of the privacy torts appear to deal directly with such problems
associated with the computerized storage of health information as
security breaches, secondary use, or distortion of data, nor do they
offer clear remedies. Despite sharing in the common law legal
tradition, Canada has not fully developed its jurisprudence in the area
of the tort for invasion of privacy.

Although not considered among the traditional privacy torts,
“breach of confidentiality” is an important dimension of “privacy,”
particularly as it relates to medical records. The idea of “privacy”
focuses on the individual’s right to be free from intrusion upon his or
her person or dignity while “confidentiality” addresses the
expectations that information shared in certain relationships, such as
the one between doctors and patients, will be held in confidence. As
courts have explained, “[o]nly one who holds information in
confidence can be charged with a breach of confidence.”

Before corporate care became the norm, patient data was

9. Id. at 264-65.
10. Id. at 265 (quoting RESTATEMENT (SECOND) OF TORTS § 652D cmt. B, (1997);
see also Goordt v. Tribune Entm’t Co., 106 F.3d 215, 220 (7th Cir. 1997)).
11. Abrial & Cava, supra note 8, at 264.
12. Id. at 265.
13. See John D.R. Craig, Invasion of Privacy and Charter Values: The Common-
14. See Neil M. Richards & Daniel J. Solove, Privacy’s Other Path: Recovering
15. Id. at 174.
16. Nicolas P. Terry, What’s Wrong With Health Privacy, 5 J. HEALTH & BIOMED.
L. 1, 6 (2009) (quoting Humphers v. First Interstate Bank of Or., 696 P.2d 527, 530
(Or. 1985)).
protected by the physician-patient relationship, violations of which could be remedied through the theory of “breach of confidence and operationalized through implied contract or tort doctrines.” With the increase of managed care, however, “access to the patient’s health file is not brokered by the treating physician in their role as confidant... [and] rarely will any one functionary act as ‘gatekeeper’.” Because the managed care system requires many people to have regular access to patient records – including health administrators, insurance companies, employers, regional health database organizations, and information brokers – monitoring and regulating the flow of patient information has become more difficult. This is especially true because “[t]he duty of confidentiality arising at the point of clinical care or research simply does not convey a right to confidentiality in all these important contexts.” Thus, in the corporate healthcare context, the traditional confidentiality model may not offer broad enough protection for patients against unauthorized disclosures of their medical information. It may be difficult, for example, to use breach of confidentiality to address problems such as hacking or regulating how information is used once it has been passed on to approved secondary users.

In some ways, unauthorized secondary use of patient information “resembles breach of confidentiality, in that there is a betrayal of the person’s expectations when giving out information.” However, breach of confidentiality is “not well suited to protecting a person’s interests in knowing when personal information will be collected and for what purposes, nor has the theory been developed as a remedy for inadequate controls over storage or security of information, or to prevent discrimination on the basis of a person’s health status.” Technology has centralized health care information, and this has increased patients' fear over who will gain access to that information and for what purposes. These concerns are often expressed in terms of “privacy,” but, in many ways, they really reflect individuals' desires to maintain control over personal data.

17. Id. at 23.
20. Solove, supra note 2, at 522.
21. Magnusson, supra note 18, at 682.
In many instances, once a patient's information has been collected, he or she is excluded from the decisions about how personal data is used.\textsuperscript{22} Although people may be aware, upon disclosure, that their personal information will be used for purposes beyond that for which it was initially collected, technology allows for secondary uses far beyond those that patients (or even doctors) anticipate upon disclosure and for which they may not have consented if they had known of them.\textsuperscript{23} However, because American courts have not recognized exclusion from such decisions as a cognizable harm, there is no tort remedy for such situations.\textsuperscript{24} It would be inefficient, as well as burdensome, on many legitimate uses to require patients' consent every time their medical information is either accessed or transmitted. Yet, it would be imprudent or even dangerous to entirely sacrifice individual autonomy in the decision process.

III. Constitutional Interpretations of the Right to Privacy

A. U.S. Constitutional Framework

In 1965, in \textit{Griswold v. Connecticut}, the Supreme Court held that it was unconstitutional for the government to prohibit married couples from using contraceptives.\textsuperscript{25} While acknowledging that the word "privacy" cannot be found anywhere in the Constitution, the Court nevertheless concluded that the Constitution provides a "right to privacy."\textsuperscript{26} The Court explained that "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that helped give them life and substance. Various guarantees create zones of privacy."\textsuperscript{27} Thus, a right to privacy can be found as an extension of a fundamental right, such as liberty.\textsuperscript{28} Then, in 1972, in \textit{Eisenstadt v. Baird}, the Court extended the reasoning in \textit{Griswold}, holding that the government also could not prevent unmarried people from using contraceptives.\textsuperscript{29} The Court emphasized

\begin{footnotesize}
\begin{enumerate}
\item[22.] Solove, \textit{supra} note 2, at 523-24.
\item[23.] \textit{Id.} at 521-22.
\item[24.] \textit{Id.} at 524.
\item[26.] \textit{See id.} at 484-85.
\item[27.] \textit{Id.} at 484 (citation and emphasis omitted).
\item[28.] \textit{Id.} at 485.
\end{enumerate}
\end{footnotesize}
that "[i]f the right to privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child."\textsuperscript{30}

A year later, in \textit{Roe v. Wade}, the Court held that a right of privacy included a "woman's decision whether or not to terminate her pregnancy."\textsuperscript{31} Instead of relying on the \textit{Griswold} and \textit{Eisenstadt} reasoning that the Constitutional right of privacy comes from "penumbras" of the Bill of Rights, the \textit{Roe} Court grounded the right in the Due Process Clause of the Fourteenth Amendment. The Court held that a woman's personal liberty protects her from state intervention in abortion decisions until the state interest in protecting the health of the mother and the potential life become "compelling."\textsuperscript{32} \textit{Roe}, therefore, also protects a kind of privacy in decision making independent of outside governmental pressures. But it does not seem to address whether the U.S. Constitution offers a right of privacy that protects personal information.

In several other cases, however, the Supreme Court has more closely addressed this latter issue. In 1977, the Court extended the constitutionally protected "zone of privacy" beyond the "interest in independence in making certain kinds of important decisions" to include an "individual interest in avoiding disclosure of personal matters."\textsuperscript{33} Here, the Court upheld a New York law that mandated doctors to report all prescriptions for certain drugs, along with other patient-specific information, which would then be entered into a centralized state computer record.\textsuperscript{34} To reach its decision, the Court considered both the individuals' interest in avoiding disclosure of personal matters and their interest in independently (without government intervention) making certain important kinds of decisions.\textsuperscript{35} Weighed against the state's need to protect the public's health and to deter criminal activity, however, the Court found that the potential harm of disclosing individuals' personal information was not a serious enough threat to either of the privacy interests to

\begin{itemize}
\item[30.] \textit{Id.} (emphasis omitted).
\item[32.] \textit{Id.} at 154
\item[34.] \textit{Id.} at 591, 606.
\item[35.] \textit{See id.} at 605.
\end{itemize}
establish a constitutional violation.\textsuperscript{36}

In \textit{Ferguson v. City of Charleston}, the Supreme Court again considered constitutionally founded rights of privacy and their applicability to medical records.\textsuperscript{37} The central issue in \textit{Ferguson} was whether a state hospital policy requiring staff to test pregnant patients for drug abuse and to report positive findings to the police violated the Fourth Amendment. The Court held that the "special needs" doctrine did not exempt the drug tests administered by the hospital from the Fourth Amendment's general prohibition against nonconsensual, warrantless, and unfounded searches.\textsuperscript{38} In this case, the Court noted that "the unauthorized dissemination of such results to third parties" represented an intrusion on privacy more serious than using adverse test results to disqualify individuals from a "particular benefit, such as a promotion."\textsuperscript{39} As the Court explained, "[t]he reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."\textsuperscript{40} Thus, the Court recognized that patients have an "expectation of privacy" that includes a guard against disclosures to certain third parties without consent.\textsuperscript{41} This, however, does not necessarily provide patients with protections from hackers or from the aggregation or manipulation of data by secondary users.

Even if U.S. courts reach a consensus on whether either the Fourth or Fourteenth Amendment guarantees a clear right to privacy of medical records, "[a]ny right to privacy under the federal or state constitutions is, of course, limited to state action."\textsuperscript{42} Because the majority of the U.S. healthcare system is privatized, this renders "a constitutional privacy protection of medical records less potent," and thus, presents only "a partial solution to the problems surrounding medical information privacy."\textsuperscript{43} This leaves a significant gap that should be filled by statutory means.

\textsuperscript{36} See \textit{id.} at 601.
\textsuperscript{38} \textit{id.} at 85-86.
\textsuperscript{39} \textit{id.} at 78.
\textsuperscript{40} \textit{id.}
\textsuperscript{41} \textit{id.}
\textsuperscript{42} Gostin et al., supra note 19, at 12.
B. Canada’s Constitutional Framework

In contrast, Canada has a more universal healthcare system. As a result, a constitutionally protected privacy right in personal health information may play a bigger role in shaping the privacy standards in the context of electronic medical records.

Canada’s Constitution, unlike that of the U.S., incorporates many documents. The Constitution Act of 1982 sets out the Canadian Charter of Rights and Freedoms ("Charter"). Although the Charter does not explicitly contain a right to privacy, the Canadian Supreme Court, like the U.S. Supreme Court, has recognized an implied right of privacy. In particular, the Canadian Supreme Court has relied on section 8 (s. 8) of the Charter, which provides individuals a right to be secure against unreasonable search or seizure, for establishing broad privacy protection.

As the Canadian Supreme Court explained in R. v. Dyment, "[s]ection 8 is concerned not only with the protection of property but also with the protection of the privacy interests of individuals from search or seizure." In Dyment, the Canadian Supreme Court found that s. 8 rights had been violated when a doctor treating a patient after a car accident drew blood that he then gave to a police officer without the patient’s consent or knowledge.

To reach this decision, the Canadian Supreme Court relied on its earlier interpretation of the Charter in Hunter v. Southam Inc. where it found the Charter provides "unremitting protection of individual rights and liberties." The Canadian Supreme Court further reasoned that:

a major, though not necessarily only, purpose of the constitutional protection against unreasonable search and seizure under s. 8 is the protection of the privacy of the individual. ... And that right, like other Charter rights must be interpreted in a broad and liberal manner so as to secure the citizen’s right to a reasonable expectation of privacy against governmental encroachments. Its spirit must not be constrained by narrow legalistic classifications based on notions of property and the like which served to protect

46. Id.
47. Id.
Although recognizing that the right to be free from unreasonable search and seizure was "rationalized in terms of property interests," the Canadian Supreme Court held that these traditional common law origins did not restrict protection and application of s. 8's "broad and general right." The Canadian Supreme Court, however, did emphasize that this right may not be absolute, as it must "be balanced against societal needs, and in particular law enforcement, and that is what s. 8 is intended to achieve." Thus, s. 8 of the Canadian Charter of Rights and Freedoms resembles the protection afforded U.S. citizens in the Fourth Amendment. Both the U.S. and Canadian Supreme Courts, therefore, have accepted that a Constitutional protection against unreasonable search and seizure provides individuals with a "reasonable expectation of privacy." This concept of privacy found in the Fourth Amendment and s. 8 appears to equate the value of privacy with liberty or the right to be free from government intrusion to the greatest degree possible while balancing the needs of society at large. Privacy conceived of in terms of liberty appears primarily to be concerned with an individual’s relationship with its government.

After holding that the freedom from state intrusion under s. 8 is broad, the Canadian Supreme Court has identified three zones of privacy over which, it is presumed, individual members of society exercise control: personal space, dignity, and personal information. The Canadian Supreme Court recognized that privacy as it relates to information, as with privacy of the person, is "based on the notion of the dignity and integrity of the individual." To further define this zone of informational privacy, the Canadian Supreme Court looked to the Privacy Commissioner's interpretation that "[t]his notion of privacy derives from the assumption that all information about a

50. Id. (citing Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.)).
51. Hunter, 2 S.C.R at 158; see also Dyment, 2 S.C.R. at 427.
52. Dyment, 2 S.C.R. at 428; see also Hunter, 2 S.C.R at 159-60.
53. Ferguson v. City of Charleston, 532 U.S. at 78; Dyment, 2 S.C.R. at 428 (citing Hunter, 2 S.C.R at 159-60).
55. Id. at 392.
person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit.”

For both the Canadian Supreme Court and the Federal Privacy Commission, the right to control the manner in which one’s personal information is used forms a critical part of one’s dignity. And the right to privacy is, at least partly, a right to maintain that personal dignity.

In *Dyment*, the Canadian Supreme Court went on to explain that:

> In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the person to whom, and restricted to the purposes for which it is divulged, must be protected.

Here, the Canadian Supreme Court recognized that people must frequently disclose personal information in the modern world, but it also emphasized that this does not mean all expectations of privacy are gone. Instead, the Canadian Supreme Court highlighted that despite the increased flow of information, individuals still retain an ongoing interest in their personal information that deserves protection.

In *McInerney v. MacDonald*, the Canadian Court emphasized that it is of “primary significance” that the nature of the information contained in an individual’s medical record is highly private and personal. As the Court observed, “[i]t is information that goes to the personal integrity and autonomy of the patient.... [S]uch information remains in a fundamental sense one’s own, for the individual to communicate or retain as she or he sees fit.” The Court also noted the fiduciary nature of the doctor-patient relationship, explaining that “information about oneself revealed to a doctor acting in a professional capacity remains, in a fundamental sense, one’s own.... The confiding of the information to the

---

57. *Id.* (quoting Dep’t. of Justice of Canada, Report of the Privacy Task Force, *Privacy and Computers* 13 (1972)).
61. *Id.*
62. *Id.*
physician for medical purposes gives rise to an expectation that the patient's interests in and control of the information will continue.\textsuperscript{63} Again, the Court considers privacy as the right to shape one's persona by controlling how one's personal information is used. This right is not lost upon disclosure to a medical professional.

As the above suggests, informational privacy is viewed as a consent-based right. Patient privacy in relation to medical records, therefore, is expressed through the right to take part in decisions regarding their personal health information. The Canadian Supreme Court seems to focus on patient control and autonomy as fundamental elements of informational privacy, mandating patients to retain some degree of control over their health information. As one commentator explained, "a patient's privacy rights in regard to his health information are respected if he has an opportunity to exercise some control over it by consenting to, or withholding consent for, various uses or disclosures."\textsuperscript{64} While the Canadian Supreme Court uses the words "control" and "autonomy," this language appears to be absent in the U.S. Constitution case law regarding privacy.

\section*{C. Comparison of the U.S. and Canadian Constitutional Approaches}

The right of privacy in the \textit{Roe} line of cases established that the Constitution protects a certain kind of decisional freedom. That is, the law recognized that the constitutionally protected concept of "liberty" encompasses an individual's right to make certain choices independently, free from outside governmental intrusion. This constitutional right of privacy, however, does not offer the individual control or protection over the collection or electronic storage of personal information or how it is used. Thus, the \textit{Roe} concept of the right to make certain decisions in "privacy" does not afford patients a guarantee of control over their personal health information once they have made the initial decision to disclose that information to healthcare providers. The Canadian cases, in contrast, seem to more fully support a constitutional privacy interest in health information that continues even after disclosure.

The American constitutional concept of privacy seems to focus

\textsuperscript{63} \textit{Id.} at 150-51 (emphasis added).

on the relationship between individuals and government and on establishing the appropriate permissible level of government intrusion in the private sphere. It is only when government goes too far, compromising an individual’s constitutionally protected right of liberty, that a privacy invasion occurs. Canadians, it seems, perceive their privacy somewhat differently, emphasizing personal autonomy. They believe that members of society should be free to decide for themselves what is important to keep under their own control. As much of the language above suggests, Canada views personal dignity as a key part of the right to privacy. In this way, the Canadian concept of privacy more closely resembles the European view, in which privacy is considered a fundamental human right. This is reflected in many international conventions on the subject. As one scholar explained, “[t]he influence of international law on Canada’s privacy regime has been felt at the most fundamental level, in helping us define our rights.”

This consent-based model, however, can raise issues in the electronic health records (EHR) context because achieving meaningful consent is often difficult. As one scholar remarked, “But how far does individual autonomy and control... extend to collection, use and disclosure of one’s health information, particularly for the purpose of providing care?” As both the U.S. and Canada face the privacy issues resulting from electronic health records, both legal systems will have to reevaluate or rebalance a patient’s autonomy (as expressed through consent and control) against the need for information to move quickly and freely within the healthcare world. This will no doubt prove challenging in both systems, though for somewhat different reasons.

IV. Federal Privacy Regulation

A. U.S. Federal Regulation of Privacy

Traditionally, in the U.S., state law has governed the protection of health care records, but as technology made EHR a reality, Congress recognized the need for, and benefits of, a more uniform

67. Id.
68. Ries, supra note 64, at 688.
approach to health care records. In 1999 Congress passed the Health Insurance Portability and Accountability Act (HIPAA). The focus of HIPAA was to establish national standards for electronic health care transactions that allowed for the more efficient flow of health information while providing security measures to ensure the privacy of health data. As Congress was unable to meet its self-imposed deadline for passing enabling legislation, the Department of Health and Human Services (HHS) developed its own set of regulations for electronic medical record transaction and storage, the Privacy Rule, which came into effect in December 2000.

The Privacy Rule applies only to certain “covered entities.” These include: health plans, health care clearinghouses, and health care providers who transmit health information electronically. The Privacy Rule places limitations on how covered entities can use and when they can disclose “individually identifiable” or potentially identifiable health information in any form – electronic and paper. The HHS regulations define this “Protected Health Information” (PHI) as including any data held or transmitted by a covered entity which concerns health status, provisions of health care, or payment for health care that can be linked to an individual. The Privacy Rule obligates covered entities to follow certain procedures and to take security measures designed to ensure that PHI remains as private as possible.

HIPAA was intended to combat the patchwork approach to health information privacy, but it fails in several crucial ways to truly provide a national privacy standard. First, the Privacy Rule does not apply to all healthcare organizations handling medical records. Second, HIPAA acts solely as a regulatory floor; federal standards only preempt those state privacy regulations that offer patients less stringent protection than those provided by HIPAA, and those that

70. See Gostin & Hodge, Jr., supra note 1, at 1459, 1466.
71. Id. at 1458.
77. Id. at 343.
conflict with federal regulations. This partial preemption rule may make compliance cumbersome in certain situations in which more than one set of privacy obligations applies, such as, for example, patients receiving treatment in several different states. This, coupled with the fact that the Privacy Rule does not apply to all healthcare organizations handling medical records, reduces HIPAA’s effectiveness measures in protecting patient privacy from harms created by technology. In addition, the absence of standards applicable across the nation perpetuates a certain level of inefficiency. For instance, it is difficult for healthcare providers to realize the full benefits of electronic health records systems. These fundamental problems with HIPAA ultimately may hinder “[e]fforts to move toward nationwide use of electronic medical records and related information technology False.”

The Privacy Rule charges covered entities with keeping PHI confidential, but the regulations also recognize various lawful secondary uses, reflecting “[t]rade-offs between public good and personal privacy.” In addition, covered entities may disclose PHI to outsiders without prior patient consent under the following circumstances and purposes:

1. to law enforcement officials
2. to judicial and administrative proceedings for commercial marketing purposes
3. to parents of unemancipated minors
4. to “significant others,” such as family members, close friends, or designated persons, of an adult or emancipated minor
5. to an authorized public health authority and for health research

As originally drafted, the Privacy Rule favored patient control. The Bush amendments, in contrast, gave healthcare providers more freedom to use and disclose patient information without first obtaining written consent. Initially, the Privacy Rule gave

78. Id.
80. Gostin et al., supra note 19, at 16.
81. Id. at 16-17; see also 45 C.F.R. § 164.512 (2010).
individuals the right to withhold consent in order to prevent their personal health information from being used or disclosed for even routine purposes.\(^83\) However, covered entities can now disclose PHI without prior patient consent for purposes relating to "treatment, payment, or healthcare operations."\(^84\) In addition, a covered entity may lawfully provide PHI to a "business associate" (e.g., corporations such as law or accounting firms with a business relationship with a covered entity), to use for routine purposes without patients' knowledge or consent and even against their will.\(^85\) This could lead to various abuses of personal rights.

The Privacy Rule attempts to strike a balance between the patient's right to maintain control over personal information, healthcare providers' need to be able to access information quickly and efficiently, and other secondary uses such as research. The difficulty lies in determining exactly how the law ought to evaluate these valid but often competing interests. Further, a certain degree of patient autonomy must inevitably be sacrificed regardless of exactly how the balance is struck.

Even when patient consent is not required prior to disclosures, the Privacy Rule instructs covered entities to notify patients that their medical information will be disclosed and how it will be used.\(^86\) This again reflects a shift away from a model emphasizing full patient autonomy and informed consent, which seriously limits the degree of control patients possess over the uses of their medical information after the initial disclosure.

Consistent with this trend, the Bush amendments have defined what constitutes impermissible "marketing" more narrowly than the initial rule, favoring commerce and corporate interests over confidentiality.\(^87\) This means that prior patient authorization is often not needed for communications related to health products or services.\(^88\) It is thus easier for commercial enterprises such as a pharmaceutical company to obtain a patient's prescription history and to send him or her unsolicited promotions of health-related products, regardless of whether this individual wishes to receive this

83. Id. at 383.
84. 45 C.F.R. § 164.506(c)(1) (2010).
86. 45 C.F.R. § 164.502(i) (2010).
87. Markey, supra note 82, at 382-85.
88. Id. at 393.
information. The resulting flood of junk mail and email spam becomes another unwanted source of intrusion into one's private life for which one has no clear remedy. The disclosure exceptions for commercial marketing, therefore, can lead to breaches of privacy; yet this loss of autonomy does not appear to be in exchange for any important public purpose.

When a covered entity discloses PHI for a permissible purpose, the Privacy Rule imposes a “minimum necessary” standard that limits the amount of information that may be disclosed. The amount of PHI revealed must not exceed the amount reasonably necessary to accomplish the purpose of the disclosure. Therefore, the patient's full medical record may not be disclosed when only certain information in the record actually pertains to the purpose of the disclosure. If individual health information can be redacted, such that it cannot be linked to a particular patient, covered entities are permitted to use and to disclose the information without authorization or any other permission specified in the Privacy Rule. When taken together, “these measures can enhance patient autonomy and promote trust in the health care system.”

However, the above safeguards may prove too weak to be convincing or reassuring. Extending the permissible disclosures to include business associates and allowing more uses to be exempt from the “marketing” restriction rapidly increases the number of potential people who could view and use individuals' health information without either their consent or knowledge. This also expands the opportunity for misuse of personal health data, as “the ability to consolidate and call in data from disparate locations in a distributed network may mean that there is no permanent database under the control of any one entity: data will simply travel as required between authenticated users of the system.”

To many, the perceived or actual danger lies in the possibility of improper use by approved users of the system or the aggregation of one's personal information from a variety of authorized sources. Unfortunately, as data can spread so quickly, a model that is
primarily concerned with patients’ rights in relation to consent to disclosure of their medical information would be impractical for both patients and healthcare professionals and would not address the most pressing privacy issues. Thus, in the electronic world, “health privacy laws must focus not on people, nor records, but on health data, including . . . conditions for the transmission and storage of data.”

Although encrypting personal information prior to transmission and creating access practices enhances patient confidentiality, “one ‘hack’ into the system, or one error by a data administrator, may compromise more data, as well as the records of a larger number of people.” The scale of the risk involving electronic medical record systems, therefore, is huge.

The protections offered by the HIPAA Privacy Rule often appear “more like a catalogue of exceptions” than a comprehensive grant of authority that allows individuals to maintain the primary control over when and to whom their health records may be disclosed.

B. Canada’s Regulation

In Canada, at the federal level, several important laws exist which are designed to safeguard informational privacy. In 1983, Canada passed the Privacy Act to “protect the privacy of individuals with respect to personal information about themselves held by a government institution.” The Act also provides individuals with a right of access to that information. The Canadian Privacy Act defines personal information broadly as: “information about an identifiable individual that is recorded in any form.” As the Supreme Court of Canada emphasized, “[t]he language is deliberately broad and entirely consistent with the great pains that have been taken to safeguard individual liberty. Its intent is to capture any information about a specific person, subject only to specific exceptions.” Unlike in the U.S., where the general federal privacy legislation does not apply in the healthcare context, the Canadian Privacy Act does offer protection for some personal health information. This significant

95. Id.
96. Id.
99. Id. (emphasis added).
difference results from the fact that the U.S. healthcare system is
tirely privatized and thus is beyond the reach of legislation
designed to regulate federal governmental action. In contrast, since
Canada has a universal healthcare system, the federal Privacy Act
does have some impact on how privacy of health records is addressed.

Recognizing an additional need to consider privacy issues in the
private as well as public sector, Canada enacted Personal Information
Protection and Electronic Documents Act (PIPEDA) in 2000. PIPEDA
regulates how private sector organizations collect, use, and
disclose personal information while engaging in “commercial
activities.” Although healthcare is for the most part publicly
funded, private healthcare providers do exist. These providers,
however, fall under the PIPEDA regulations because the funding
source does not determine whether an activity is designated
“commercial” or not. An individual’s health information is
regulated by the Privacy Act or PIPEDA, depending on whether the
healthcare provider is a government institution or a private actor.
In Canada, as in the U.S., the absence of a single piece of privacy
legislation applicable to every healthcare professional means
protection of personal health information varies somewhat. This may
prove problematic because for the full benefits of electronic health
records to be realized, a uniform approach to protection health data
seems preferable. Uniformity would contribute both to making the
flow of health information more efficient and to convincing patients
that their information is well protected.

PIPEDA introduced measures to protect personal information in
the private sector. In order to ensure effectiveness, it establishes
broad privacy protection and specifically includes protection of
information in electronic form. To achieve this, PIPEDA lays out a
number of basic principles: accountability, identifying, purpose,
consent, limiting collection, limiting use, disclosure and retention,
accuracy, safeguards, openness, individual access, challenging
compliance. All personal information collected, used, or disclosed
in connection with a “commercial activity” must be regulated in such

101. Personal Information Protection and Electronic Documents Act, 2000 S.C.,
ch. 5 (Can.) [hereinafter PIPEDA].
102. Id., ch. 5, § 4(1)(a) (Can.).
103. Ries, supra note 64, at 692.
104. PIPEDA, 2000 S.C., ch. 5, § 4 (Can.).
105. See Ries, supra note 64, at 692.
a way as to conform to these basic privacy principles. Although the Canadian approach to federal level privacy regulation of the private sector has the advantage of offering uniform guidelines, it still does not guarantee uniformity in how these privacy principles are implemented.

Thus, PIPEDA offers a co-regulatory model: the industry develops the specific standards and implements them while these standards are overseen by the governmental privacy agency to ensure compliance with the overarching private sector-wide privacy scheme. In the U.S., there is no comparable overarching privacy legislation that protects personal information in the private sector. This has proven to be problematic. Instead, at the federal level, the U.S. has addressed privacy issues through industry-specific legislation, such as HIPAA. This may provide certain advantages. For instance, the industry-specific approach may afford greater privacy protection because of the specificity inherent in legislation geared at a single subject area. This may be especially beneficial in regard to the highly sensitive nature of personal medical data. For example, the comprehensive laws in Canada do not define what information is "sensitive," merely stating instead that "any information can be sensitive, depending on the context." In some ways, this definition creates more ambiguity because HIPAA clearly targets personal identifiable health information. At the same time, PIPEDA's more flexible definition of "sensitive" information may allow for broader protection.

Although PIPEDA provides a broad privacy protection scheme, as noted above, it does not successfully combat the problems of patchwork regulation. Notably, it allows the Canadian federal government to exempt organizations or commercial activities in provinces which have privacy laws deemed "substantially similar" to the federal law. In fact, Alberta, British Columbia, and Quebec

109. Id.
110. PIPEDA, 2000 S.C., ch. 5 (Can.).
111. PIPEDA, 2000 S.C., ch. 5, § 26(2)(b) (Can.); see also Substantially Similar Provincial Legislation, OFF. OF THE PRIVACY COMMISSIONER OF CANADA, http://www.priv.gc.ca/legislation/ss_index_e.cfm#content top (last visited Sept. 18,
have enacted such laws; thus the private sector in those provinces is subject to those specific privacy laws rather than to the federal standards. This structure resembles the U.S. system. HIPAA always acts as a regulatory floor, but in those states which have enacted more stringent medical privacy laws, the stricter laws will govern medical transactions. Thus, in both Canada and U.S., federal laws do not completely preempt state or province regulation in the area of medical privacy.

A key difference, however, is that, unlike HIPAA, PIPEDA seems to promote greater uniformity in privacy legislation because of the “substantially similar” requirement that must be met. HIPAA contains no such analogous provision; it does not mandate any degree of similarity between the state medical privacy laws and the federal regulations. Instead, HIPAA requires that state law merely offer the patient a higher degree of privacy protection than that in HIPAA. It does not, however, specify the form or content of these regulations. This leaves a high level of ambiguity, imprecision, and confusion for healthcare professionals and patients in a particularly sensitive area, namely, human rights. Thus, the Canadian law seems to be moving more directly toward the establishment of a true national standard for privacy protection.

The current U.S. legislation does not explicitly appear to be striving for a national scheme, at least in the significant area of establishing some kind of general privacy protection for personal information in the private sector. This shortfall may, in part, result from the fact that the U.S. does not traditionally regulate the private sector as it would conflict with our prevailing notions of a free-market economy. As a result, the U.S. approach to data privacy, in contrast to the Canadian approach, must rely in great measure on self-regulation, largely based on company or industry-wide self-imposed or aspirational standards. Therefore, comprehensive privacy legislation will likely continue as only industry-specific. This could


113. Gostin & Hodge, Jr., supra note 1, at 1465-66.


115. Id.
shackle the development of a fair and enlightened policy for some time.

The Canadian federal government has demonstrated its commitment to safeguarding electronic health records through its funding of a not-for-profit organization, Health Infoway. Its purpose is to work with the provinces and territories to foster and accelerate the development and adoption of pan-Canadian electronic health information systems. This comprehensive system will likely help address some privacy issues resulting from electronic transmission of sensitive information by creating a uniform approach to security and privacy expectations; but it may not adequately safeguard secondary uses or aggregation of personal data. Despite the potential benefits a structure of this kind affords, the fundamental differences between the U.S. and Canadian healthcare parameters and attitude toward free-markets makes it unlikely that U.S. could ever develop a comparable plan. Because the U.S. healthcare system will likely continue to be largely owned and operated by various private entities, security measures and privacy standards will be harder to implement in the U.S.

Canada's privacy regime differs from that of the U.S. in another important aspect: Canada has established a Privacy Commission and Commissioner, who is responsible for enforcing federal privacy laws. The Privacy Commissioner operates independently, separate from the Prime Minister's cabinet, and he or she reports directly to the Canadian House of Commons and the Senate. The Commissioner has the power to investigate complaints brought by individuals, to conduct audits under the two federal laws, and to publish reports about personal information handling practices in both public and private sector. The U.S. has no consolidated agency strictly dedicated to dealing with privacy issues across the industries and private sector. In addition, HIPAA and the Privacy Rule do not give individuals a private right of action. Instead, enforcement of the Privacy Rule is left to HHS's Office for Civil Rights and the

117. Id.
118. See Canada Privacy Act, R.S.C., ch. P 21 (1985); see also PIPEDA, supra note 102, at ch. 5 § 4.
120. Id.
Department of Justice.121

Although the U.S. constitutional and common law approaches to privacy and confidentiality “suggested a rights-based approach to legal confidentiality that paralleled the autonomy principle,”122 HIPAA represents a major shift in emphasis. This seems again to undermine patients’ sense of control over their personal health information. Thus, significantly, in the U.S., “[r]ights for individuals to control their information,’ . . . have a less certain future.”123 As commentators have observed, “the federal standards have gutted the nascent rights-based approach to privacy and confidentiality, preferring . . . [a] rationale that is almost totally focused on institutions and compliance.”124 Canada, in marked contrast, appears to be continuing, in both its legislation and common law jurisprudence, to pursue a more consent-rights driven approach to protecting personal health information. Ultimately, which approach will prove to offer patients the greatest protection against the dangers of unauthorized access and secondary uses remains to be seen.

V. Conclusion

The laws in both the U.S. and Canada have recognized the need to balance individuals’ privacy with the common good. Therefore, like many rights, privacy is not absolute. Courts and legislatures constantly struggle to address the needs of society without entirely compromising those of the individual. As technology continues to develop, the balancing becomes increasingly complex and difficult. Electronic record keeping presents exciting possibilities for healthcare to be delivered in a more organized and effective manner. It also has the potential to offer patients more security for their medical records and ensure a greater degree of accuracy and accessibility, thus improving overall care. But, because such centralized systems contain large amounts of personal data, including information about a patient’s mental and physical health, social behaviors, and employment and financial status, protecting the privacy of health data is critical. Without adequate safeguards for

121. 45 CFR §§ 160.300-160.312 (2010); If a complaint describes an action that potentially violates criminal provision of HIPAA (42 U.S.C. 1320d-6), OCR can refer it to the DOJ.
122. Magnusson, supra note 18, at 688.
123. Id.
electronic records, health information can become subject to unauthorized access, disclosures, and unwelcome secondary uses, potentially leading to social stigma and discrimination by insurance companies, healthcare professionals, and institutions, as well as employers. Patients need and want to feel that they have control over the use and circulation of their personal information and appropriate protection against the harmful consequences caused by the use or disclosure of their personal health information. Whether or not the fear that electronic medical records compromise privacy is well-founded, it nevertheless remains essential that patients believe that their personal information is secure. Otherwise, they may be reluctant to communicate openly with healthcare professionals, causing harm to themselves and impeding important public health functions and research. Thus, there is also a communal benefit to ensuring privacy.

What constitutes a violation of privacy, and what harms occur as a result of such violations, is not static. Technology in particular is reshaping how developed countries view privacy, while continually presenting new privacy dilemmas. For instance, aggregation of data can link together information which, independently is insignificant, but together is compromising. Thus, the law must create a privacy framework flexible enough to continually reevaluate the balance between patient privacy rights and the societal need to collect information.

As Canada shares with the U.S. a language, a common law legal tradition, and a similar geographic size and political structure, examining Canada's approach to this complex privacy problem could potentially offer the U.S. some alternative ways of addressing it. Although clearly Canada's system also has its shortcomings, several differences seem noteworthy. Perhaps most strikingly, Canada has set up a Privacy Commission and Commissioner to oversee the implementation of federal privacy regulations. The merits of this innovation include streamlining consistency and compliance, providing individual citizens with a clear remedy, and establishing straightforward checks and balances. Also, because healthcare is largely a public operation in Canada, this somewhat simplifies the issues there. For example, privacy regulations that restrict the federal government automatically apply to healthcare. All these elements may help promote trust in the system. In addition, Canada's PIPEDA offers broad privacy protection across the private sector, something the U.S. currently lacks.
In the end, neither country has yet addressed the current challenges with complete success: How to adequately protect individuals from the new harms of widespread availability of centralized electronic records while simultaneously developing the full potential benefits of keeping accurate and comprehensive data. The importance of this issue for human rights and human health make it imperative that we continue to search for a satisfactory legal framework that achieves these goals. A stance of open-mindedness, creativity, and flexibility will be necessary to accomplish this goal.
***