HIPAA IN THE AGE OF ELECTRONIC HEALTH RECORDS

Eric S. Pasternack*

I. INTRODUCTION

Advances in computer technology soon promise to alter the medical profession in a fundamental way. For years now, many have predicted and worked to develop electronic health records. More recently, Presidents George W. Bush and Barack H. Obama have championed the adoption of electronic health records, and corporations such as Google and Microsoft have launched platforms designed to increase the usage of such records. Theoretically, these records promise to improve the quality of the communications between patients and physicians thereby improving the efficiency and quality of care. Nevertheless, electronic health records are


4 See discussion infra Part II.
especially prone to misuse, and this is significant given the personal nature of
information they contain. As a result, Congress must act to modernize the
law to account for these technological advances, which threaten the privacy
of patient health information. To do this, Congress should amend the Health
Insurance Portability and Accountability Act ("HIPAA"), which Congress
enacted in 1996 to address the security and privacy of healthcare data. First,
Congress should expand the list of "covered entities" to include companies
that operate databases that store electronic health records ("companies").
Second, HIPAA should provide a private right of action to the victims of
security breaches. And finally, HIPAA should require those companies to
disclose information regarding security breaches to the public, thereby
fostering trust between consumers and the companies, when such trust is
warranted, while also providing an incentive for such companies to improve
their security protocols and procedures.

This Note will begin with a discussion of electronic health records in
Part II. Specifically, this section will compare traditional paper health
records to electronic health records, and it will conclude with an overview of
two popular electronic health records systems.

Part III of this Note will provide a general overview of HIPAA, and in
Part IV, this Note will discuss the need to amend HIPAA. In this section, this
Note will critique HIPAA, and it will provide a synopsis of the present
medical identity theft crisis.

Part V of this Note will address the current legal framework regarding
the regulation of electronic health records, as well as two proposals that aim
to protect the confidentiality of such records.

Finally, in Part VI, this Note will discuss my proposal to amend HIPAA.

II. ELECTRONIC HEALTH RECORDS

As the principal repository for information pertaining to a patient’s
health and healthcare-history, medical records are integral to the practice of
medicine. Traditionally, medical records were paper documents that were
passive and historical in nature, and while electronic health records are

5. See discussion infra Part III.
6. COMM. ON IMPROVING THE PATIENT RECORD DIV. OF HEALTH CARE SERVS.: INST. OF
MED., THE COMPUTER-BASED PATIENT RECORD 8 (Richard S. Dick & Elaine B. Steen eds.,
1991) [hereinafter PATIENT RECORD].
7. Steve Lohr, Health Care that Puts a Computer on the Team, N.Y. TIMES, Dec. 27,
becoming more common, paper records are at present the primary means of recording healthcare information.  

Without a single source of law governing the content of medical records, they often appear in a variety of formats, and this makes it difficult for healthcare professionals to coordinate care. Exacerbating this problem is the fact that most people have multiple medical records, with a patient usually having a record “for each health care provider they have visited.” This further impedes the coordination of care, which is noteworthy because the health care industry is “dominated’ by how well information is processed or reprocessed, retrieved, and communicated.” Furthermore, the costs associated with paper records are also significant, and the demand for patient data is increasing, thereby making this coordination problem even more acute.

Conversely, the advent of electronic health records promises to revolutionize the health care industry by providing medical professionals and patients with new capabilities and efficiencies that traditional health records cannot offer. When digitized, health records can become a “vibrant tool” that can remind and advise doctors as to the proper course of treatment.

8. Carter, supra note 1, at 7; PATIENT RECORD, supra note 6, at 13. Carter, supra note 1, at 7. For the purposes of this article, the term “paper records” connotes the full spectrum of non-electronic health records. Significantly, paper records often “appear in a variety of forms—for example, as paper; microfilm; a monitor strip; an optical disk; a computer card, tape or disk; or a combination of these . . . .” PATIENT RECORD, supra note 6, at 13.

9. There is “no one source of law [that] definitely addresses the legal requirements governing the content of medical records. Rather a myriad of sources supply these requirements: statutory, regulatory, accrediting, institutional, and professional guidelines.” DANA C. MCWAY, LEGAL ASPECTS OF HEALTH INFORMATION MANAGEMENT 67 (2d ed. 2003).

10. See supra note 8.

11. PATIENT RECORD, supra note 6, at 18 (“Paper patient records offer little hope of improving the coordination of health care services within or among provider institutions.”).

12. Id. at 12–13.

13. Id. at 19.

14. Id. Approximately “35 to 39 percent of total hospital operating costs have been associated with patient and professional communication activities. Physicians spend an estimated 38 percent and nurses an estimated 50 percent of their time writing up patient charts.” Id. (citations omitted). It has also been estimated that approximately 40% of the costs involved with running a hospital are for “storing, collecting, and moving information” associated with traditional paper health records. Paul M. Schwartz, Privacy and the Economics of Personal Health Care Information, 76 TEX. L. REV. 1, 13 (1997) (internal quotation marks omitted).

15. PATIENT RECORD, supra note 6, at 21.

16. LOHR, supra note 7. For example, computer programs “can be written to flag prior allergic reactions, drug interactions, or other contraindications for contemplated therapy, thus
Electronic health records “will allow patients to store, retrieve, manage, and share their health data—such as lists of medical problems, medical histories, medications, allergies, immunizations, test results, insurance information, and doctor’s visits—over the Internet.”

While traditional paper records contain similar information, electronic health records provide a degree of functionality that paper records cannot match. Electronic health records can be “interlinked” thereby maximizing the coordination of care, and when converted into a digital format, the accessibility of health records vastly increases. In essence, the records become merely a click away once digitized, the importance of which cannot be stressed enough, as patients “now are more likely to receive care in ambulatory [settings] rather than [in] in-patient settings.” Furthermore, the increase in “shared care,” where[] the patient shares responsibility with the care provider,” along with the fact that patients are “likely to have increasingly episodic relationships with multiple providers” contributes to the significance of the advent of electronic health records.

Additionally, by using electronic health records, the risk that a pharmacist or another health care professional will misread the records... reducing the potential for error.” Nicolas P. Terry & Leslie P. Francis, Ensuring the Privacy and Confidentiality of Electronic Health Records, 2007 U. ILL. L. REV. 681, 692 (2007). Such programs also permit “entries in patients’ records to be checked against programmed guidelines and clinical decision support systems, prompting providers if prescription amounts are out of range, if necessary data have been omitted in the record, or if the recommended procedures have not been performed.” Id. at 693. Additionally, computer systems can be designed to update health records automatically, thereby eliminating the need for medical professionals to manually update a record after a procedure or laboratory test is completed. Id.

17. Robert Steinbrook, Personally Controlled Online Health Data— The Next Big Thing in Medical Care?, 358 NEW ENG. J. MED. 1653, 1653 (2008); see also Lohr, supra note 7.
20. Lohr, supra note 7. In fact, a 1991 report by the General Accounting Office stated that “automated patient records can improve health care delivery by providing medical personnel with better data access, faster data retrieval, higher quality data, and more versatility in data display.” PATIENT RECORD, supra note 6, at 8–9.
21. Terry & Francis, supra note 16, at 694. The reason for this shift can be attributed to two changes in society. First, people today are more mobile. Id. Second, people are also more likely to change physicians as their insurance changes. Id.
22. Id. at 695. For an interesting perspective on how the increase in shared care will redefine contributory negligence, see Sharon W. Murphy, Contributory Negligence in Medical Malpractice: Are the Standards Changing to Reflect Society’s Growing Health Care Consumerism?, 17 U. DAYTON L. REV. 151 (1991).
decreases because electronic health records are inherently “legible.”23 They are also “directly transferable, thus avoiding transcription errors and delays in recording prescriptions or test results communicated by telephone.”24 Because of this, many support the widespread adoption of electronic health records. Presidents George W. Bush and Barack H. Obama have indicated their support for electronic health records, and numerous reform proposals have been introduced in Congress to increase the usage of electronic health records.25

A. Electronic Health Record Platforms

A variety of platforms are available that provide consumers with electronic health records. There are client-server systems and web-based systems,26 and while both play an important role in the development of electronic health records, this Note will only discuss web-based systems such as Google Health and Microsoft HealthVault because they typify web-based systems.

1. Google Health

In May 2008, Google officially launched Google Health,27 making it open to the public after a year and a half of development and a two-month pilot project at the Cleveland Clinic.28 According to Dr. C. Martin Harris, the Cleveland Clinic’s chief information officer, the pilot program had over 1600 patients.29 More notably, Dr. Harris claimed that the patients in the Cleveland trial “did not shun the Google health records because of qualms that their

24. Id.
25. See supra notes 2–3 and accompanying text.
29. Id. According to Dr. Harris, linking the clinic’s records to Google increased the usage of the clinic’s records. Id. It allowed “the user to send personal information, at the individual’s discretion, into the clinic record or to pull information from the clinic records into the Google personal file.” Id. And this capability is, according to Dr. Harris, useful since it would provide doctors with critical information that previously may have been omitted by patients. Id.
personal health information might not be secure if held by a large technology company."

Upon signing up for Google Health, which is free to consumers, users can store all of their healthcare information in one place. Users “can enter as little or as much information as [they] want . . .” Google even allows users to import their records and prescription histories from entities such as hospitals, labs, and pharmacies with which Google has partnered. Once users import or enter their information, Google Health checks for potential interactions between their medications and allergies. It also allows users to refill prescriptions, ask for second opinions, and obtain personalized health information based on the information contained in their records.

The central principle to Google Health’s privacy policy is that users are in control of their information. By default, users are the only ones who can view and edit their information, but they can share it with others, thereby diluting the control that users have over their information.

When users decide to share their information, Google provides them with a list of who has accessed their information, and Google allows users to revoke access to their information at anytime. Nevertheless, Google warns users that while they have the power to “revoke someone’s ability to read

30. Id.


34. Id.

35. Id.

36. Id.

37. Google Health integrates with Google’s other services, such as Google Maps and Gmail, thereby allowing users to find new doctors by either specialty or location. Id.

38. Id.


40. Id.

41. Id.

[their] health information . . . [that party] may have already seen or may retain a copy of the information.”

Google has also partnered with a number of third-party websites that are capable of transmitting patient health information to Google Health. Accordingly, “[t]hese service providers (which may include [the user’s] medical providers) may provide information about certain medical conditions or extend the functionality of Google Health in other ways.” What is noteworthy about this is that once another website accesses a user’s information, that website may store that user’s information, and once information is stored on a third-party website, the information is then governed by the third-party’s privacy policy.

In addition, Google also states on its website that it is not regulated by the HIPAA privacy rule. According to Google, “[t]his is because Google does not store data on behalf of health care providers. Instead, [Google’s] primary relationship is with the user” and it is therefore governed by Section 5 of the Federal Trade Commission Act as an alternative to HIPAA. Furthermore, Google’s privacy policy states that “[u]nder the Electronic Communications Privacy Act (ECPA), Google may not voluntarily share most user information with law enforcement.” Google also states that “[u]nder various federal and state laws, Google must share user information to comply with court orders and subpoenas.”

2. Microsoft HealthVault

In October 2007, Microsoft launched HealthVault, an online repository where users can store their health information. Thereafter, in June 2008, Microsoft began a pilot project with Kaiser Permanente, “the nation’s largest nonprofit health maintenance organization.” The pilot project was available

43. Id.
44. Id.
45. Id.
46. Id.
48. Id.
49. Id.
50. Id.
51. Id.
to Kaiser’s 156,000 employees, and it came after successful pilot projects between Microsoft and the Mayo Clinic and New York–Presbyterian Hospital.\textsuperscript{54}

At its most basic level, HealthVault was designed to be a secure repository of patient health records that U.S. users can use and manage for free.\textsuperscript{55} According to Microsoft’s website, “HealthVault offers [users] a way to store health information from many sources in one location, so that it’s always organized and available . . . online.”\textsuperscript{56} To facilitate this, Microsoft designed HealthVault to work with doctors, hospitals, employers, pharmacies, insurance providers and manufacturers of health devices so that users can easily add their health information to HealthVault.\textsuperscript{57}

Upon viewing Microsoft’s privacy policy, users are immediately presented with the TRUSTe seal,\textsuperscript{58} and the HONcode seal.\textsuperscript{59} These services provide consumers with information regarding the companies that bear their seals, and aim to aid consumers in determining what company’s services to patronize. While TRUSTe reviews Microsoft’s privacy practices, the “TRUSTe program covers only information collected through Microsoft’s Web sites, and does not cover Programs or information collected through software downloaded from the site.”\textsuperscript{60}

Like Google Health, Microsoft HealthVault provides users with control of their own health records.\textsuperscript{61} When a user utilizes HealthVault to establish an electronic health record, that user becomes the custodian of the record.\textsuperscript{62} And as the custodian of the record, the user “can add and remove other custodians and users who can view and modify the record.”\textsuperscript{63}

Since custodians possess the highest level of access, they can read the record, change the record, delete the record, and grant others access to the record.\textsuperscript{64} Custodians may even grant others custodian-level access to a

\textsuperscript{54} Id.
\textsuperscript{55} Id.
\textsuperscript{57} Id.
\textsuperscript{59} Microsoft HealthVault Account Privacy Statement, supra note 58; see also Health on the Net Foundation, http://www.hon.ch/HONcode/Conduct.html (last visited Feb. 6, 2011).
\textsuperscript{60} Microsoft HealthVault Account Privacy Statement, supra note 58.
\textsuperscript{61} Id.
\textsuperscript{62} Id.
\textsuperscript{63} Id.
\textsuperscript{64} Id.
record, and those custodians may in turn grant others custodian-level access. Furthermore, a custodian may revoke another’s access to the record, and this includes other custodians. As a result, a user may grant custodian-level access to another, who then may then revoke the original user’s access to the record.

There are two other levels of access: view-only access and view-and-modify access. What is noteworthy about these levels of access is that individuals with these levels of access may grant the same level of access to others.

III. HIPAA

In 1996, Congress enacted HIPAA to require the Department of Health and Human Services “to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers,” and to address the security of patient health information. When Congress enacted HIPAA, it “recognized that safeguards were needed to control the exchange of highly personal and confidential medical information.” To accomplish these ends, Congress delegated to the Department of Health and Human Services the power to establish national standards for electronic health care transactions. However, HIPAA does not preempt state laws, which are designed to protect health information, that are

65. Id.
66. Id.
67. Id.
68. Id.
70. Id.
71. JUNE M. SULLIVAN, HIPAA: A PRACTICAL GUIDE TO THE PRIVACY AND SECURITY OF HEALTH DATA xiii (2004). Moreover, [t]he HIPAA Privacy Rule has three major purposes: 1. To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information; 2. To improve the quality of health care in the United States by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of care; and 3. To improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals.
72. See id. at xiii.
more demanding than the standards adopted by the Department of Health and Human Services.\textsuperscript{73}

Nor is HIPAA’s focus far-reaching. Instead, the HIPAA privacy rule\textsuperscript{74} applies to only “covered entities.”\textsuperscript{75} HIPAA regulations therefore apply to only health plans,\textsuperscript{76} health care clearinghouses,\textsuperscript{77} and health care providers\textsuperscript{78}.

\textsuperscript{73} Id. at 2. What is especially noteworthy about HIPAA is that “state laws related to the privacy of health information that are \textit{more stringent} than HIPAA remain in effect, even if they are contrary to HIPAA.” Id. For example, the U.S. Department of Health and Human Services states on its website that “a State law that provides individuals with a right to inspect and obtain a copy of their medical records in a more timely manner than the Privacy Rule is ‘more stringent’ than the Privacy Rule.” Health Information Privacy: How Do I Know if a State Law is “More Stringent” than the HIPAA Privacy Rule?, http://www.hhs.gov/ocr/privacy/hipaa/faq/preemption_of_state_law/403.html (last visited Feb. 6, 2011). Additionally, “[s]tate laws that are contrary to the Privacy Rule are preempted by the Federal requirements, unless a specific exception applies.” Does the HIPAA Privacy Rule Preempt State Laws?, http://www.hhs.gov/hipaafaq/state/399.html (last visited Feb. 6, 2011). For example, state laws preempt HIPAA if they include the following exceptions:

1. relates to the privacy of individually identifiable health information and provides greater privacy protections or privacy rights with respect to such information; 2. provides for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention; or 3. requires certain health plan reporting, such as for management or financial audits. In these circumstances, a covered entity is not required to comply with a contrary provision of the Privacy Rule.

\textsuperscript{74} The privacy rule covers “protected health information” that is “created or received by a covered entity.” SULLIVAN, supra note 71, at 5 (emphasis omitted).

\textsuperscript{75} Id. at 3.

\textsuperscript{76} “A health plan is an individual or group plan that provides, or pays the cost of, medical care.” Id. (emphasis omitted).

\textsuperscript{77} A health care clearinghouse is a public or private entity, including a billing service, repricing company, community health management information system, or community health information system, and ‘value-added’ networks and switches, that does either of the following functions: [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; 2.] Receives a standard translation from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

\textsuperscript{78} “A health care provider is a provider of services, a provider of medical or health services, or any other person or organization who furnishes bills, or is paid for health care in the normal course of business.” Id. (emphasis omitted).
that transmit “health information in electronic form in connection with health care transactions.”

These regulations prohibit covered entities from disclosing protected health information without first obtaining patient authorization. However, there are exceptions that allow covered entities to disclose protected health information without first obtaining patient authorization in a narrow set of circumstances. Consequently, HIPAA does not prohibit non-covered entities, such as those organizations that operate electronic health record databases, from disclosing protected health information.

IV. NEED TO AMEND HIPAA

Since HIPAA’s regulations are limited to “covered entities,” they do not apply to companies, such as Google and Microsoft that operate electronic health records systems. Consequently, user agreements and the Federal Trade Commission Act provide the sole basis for protection afforded to consumers of such services. This is insufficient, however, as explained below.

A. Critique of HIPAA’s Privacy Rule

Obviously, the most fundamental limitation on the HIPAA Privacy Rule is the fact that it applies only to “covered entities.” Because of this, one editorial opined that: “With an Orwellian turn of phrase, the ‘privacy rule’ has little to do with patient confidentiality. In fact, it permits the widespread

79. Id. at 3.
80. “Protected health information is individually identifiable information that is recorded orally or in written form by a covered entity or received by a covered entity that relates to the past, present, or future physical or mental health of an individual, health care services, or payment for health care.” Id. at 5.
81. Id. at 6.
82. “Under some circumstances, a covered entity may disclose PHI without a patient’s authorization in order to carry out treatment, payment, or health care operations.” Id.; see HIPAA, 45 C.F.R. § 164.501 (2009). Protected health information may also be disclosed without consent if the covered entity believes that disclosure will “prevent or lessen a serious and imminent threat to the health or safety of a person or the public.” Sullivan, supra note 71, at 35–36. Furthermore, disclosures may also be made to law enforcement officials, public health officials, and in judicial proceedings in a very narrow set of circumstances. Id. at 36–42.
83. See supra notes 74–79 and accompanying text.
84. See supra notes 74–79 and accompanying text.
sharing of medical data among 800,000 or so health, business and government entities.\textsuperscript{85}

There are numerous reasons for why this is the case. First, HIPAA is almost exclusively concerned with the “process of patient consent to disclosure,” instead of “limiting the collection and dissemination of personal health information.”\textsuperscript{86} Furthermore, “although HIPAA confidentiality is premised on national standards, the confusing and operationally obstructive ‘more stringent’ partial preemption rule—the so-called HIPAA floor—undercuts this model.”\textsuperscript{87} There are also numerous “unrestricted uses of patient information outside of treatment and billing,”\textsuperscript{88} and as the number of people with access to patient information increase, so too does the risk that the security of that information may be compromised. Finally, HIPAA’s enforcement provisions are notoriously weak and undermine the legislation’s effectiveness.\textsuperscript{89}

\textbf{B. Medical Identity Theft}

An identity theft crisis has developed in recent years as computers have become more common, and this is problematic since medical identity theft is a serious threat that has the potential to undermine the widespread adoption of electronic health records. According to a survey conducted in 2007, 40% of respondents feel that the risks associated with the adoption of electronic health records outweigh the benefits.\textsuperscript{90} While fear concerning security risks threaten to undermine the adoption of electronic health records, these fears are reasonable and must be taken in account. In another study, the Federal Trade Commission (“FTC”) found that there have been 19,428 instances of medical identity theft since 1992.\textsuperscript{91} The World Policy Forum has also found that approximately a half million people have been the victims of identity theft.\textsuperscript{92} However, a study by the FTC presents a far graver picture of the

\begin{itemize}
\item \textsuperscript{85} Terry & Francis, supra note 16, at 714 (quoting Medical Privacy: A Dose of Bad Medicine, PHILA. INQUIRER, Jan. 6, 2006, at A16).
\item \textsuperscript{86} Terry & Francis, supra note 16, at 714–15 (emphasis omitted).
\item \textsuperscript{87} Id. at 715 (citations omitted).
\item \textsuperscript{88} Id.
\item \textsuperscript{89} See infra notes 176–179 and accompanying text.
\item \textsuperscript{90} The data is from a Wall Street Journal Online/Harris Interactive Survey of 2153 adults, which was conducted online in the United States on November 12–14, 2007. Steinbrook, supra note 17, at 1655.
\item \textsuperscript{91} Latour “LT” Lafferty, Medical Identity Theft: The Future Threat of Health Care Fraud Is Now, J. HEALTH CARE COMPLIANCE, Jan.–Feb. 2007, at 11, 11.
\item \textsuperscript{92} Id.
\end{itemize}
identity theft crisis, which found that approximately ten million Americans had been the victims of identity theft over a five-year period.

Likewise, anecdotal evidence paints an equally grave picture of the medical identity theft crisis. For instance, in May 2009, hackers accessed eight million patient health records in Virginia and demanded a $10 million ransom payment.94 Similarly, hackers broke into twenty separate databases that the health services center at the University of California, Berkeley operated in October 2008.95 And these hackers managed to steal social security numbers, birth dates, addresses, and immunization records from the health services center.

Besides directly affecting the victims of data breaches, medical identity theft also threatens to undermine the adoption and benefits of electronic health records by instilling fear in people that their records are not secure. “[I]nadequate privacy protection not only distorts future information exchanges between physician and patient, but endangers one popular aspect of health care reform: its emphasis on preventative medicine.”97 Employers

93. Id. at 12.
96. Id.
97. Schwartz, supra note 14, at 32. See generally id. at 7–12 (comparing the views of Judge Richard Posner and Professor Richard Epstein on the economics of data privacy). According to Posner, privacy is an “intermediate good.” Richard A. Posner, The Right of Privacy, 12 GA. L. REV. 393, 394 (1978). Thus, according to Posner, “we have two economic goods, ‘privacy’ and ‘prying.’” Id. at 394. Naturally, people “profess high standards of behavior in order to induce others to engage in social or business dealings with them.” Schwartz, supra note 14, at 8 (quoting Posner, supra, at 399). Prying, on the other hand, “enables one to form a more accurate picture of a friend or colleague, and the knowledge gained is useful in one’s social or professional dealings with him.” Posner, supra, at 395. Because of this, Posner argues that “privacy can provide a considerable obstacle to efficient marketplace transactions through its effect on the ongoing exchange of personal data that is part of social life.” Schwartz, supra note 14, at 8. Therefore, privacy protections “should be protected only to the extent to which it increases social utility and assigned away from individuals when it does not.” Id.; see also Posner, supra, at 398–401. For Richard Epstein, “unrestricted access to personal genetic data has a large potential for increase social wealth.” Schwartz, supra note 14, at 10; see also Richard A. Epstein, The Legal Regulation of Genetic Discrimination: Old Responses to New Technology, 74 B.U. L. REV. 1, 16 (1994). Therefore, for Epstein, “[s]etting legal restrictions on access to genetic information will…permit the advances of science to be ‘frittered away.’” Schwartz, supra note 14, at 10; see also Epstein, supra, at 23.
already utilize patient health information when it is available to them to deny employees jobs or promotions,\textsuperscript{98} and the costs of health care will continue to provide an incentive for employers to discriminate.\textsuperscript{99} Insurance companies likewise use patient health information to deny health care coverage to these same individuals,\textsuperscript{100} and due to this, people may either “lie to their physicians or avoid seeking care that might lead to the creation of sensitive health care or genetic information,”\textsuperscript{101} since they may calculate that risks of a data breach, which may have important ramifications for their personal and professional lives, outweighs the risks associated with neglecting necessary care. Because of this, efforts to increase the usage of electronic health records will likely either fail or succeed based upon the perceived threats to the security of those records, and without reforms to bolster their security, the benefits associated with the adoption of electronic health records may never materialize.

V. CURRENT LEGAL FRAMEWORK

The law governing the security and privacy of information is highly fragmented. In fact, “[t]here is no single law, statute, or regulation that governs a company’s obligations to provide security for its information.”\textsuperscript{102} Rather, there currently exists a patchwork of laws—both common law and statutory—that govern the security of information.\textsuperscript{103}

A. Statutory Framework

There are dozens of statutes that impose obligations on corporations and individuals to provide security for information.\textsuperscript{104} These laws essentially fall into the following categories:

- [1] Privacy laws and regulations that require companies to implement information security measures to protect certain personal data they maintain about individuals;
- [2] E-transaction laws designed to ensure the

\textsuperscript{98} Schwartz, supra note 14, at 3.
\textsuperscript{99} Id. at 26.
\textsuperscript{100} Id. at 3.
\textsuperscript{101} Id. at 22.
\textsuperscript{103} Id.
\textsuperscript{104} See generally id. at 71–80.

Although these laws define the security obligations in nebulous “terms such as ‘security’ or ‘safeguards,’” none of them apply specifically to the use of electronic health records by companies such as Google and Microsoft, which are not “covered entities” under HIPAA.

B. Common Law

Numerous court decision and commentators now accept that there might be a common law duty to provide security for information. While the acceptance of such a common law duty to provide security for information is a positive step forward for privacy advocates, there are numerous flaws with a common law approach, since the “legal system is ill-suited to provide redress to the online networker.”

First, litigation is inherently “costly and time consuming.” It also may be “counter-productive,” since litigation may result in “unwanted attention to the damaging information and incorporate it into the public record.” The fact that “monetary damages are hard to prove, as they commonly involve unquantifiable injury to reputation and dignity” will also likely hinder the effectiveness of litigation as a tool to protect the privacy of patient health information. There may also be jurisdiction issues that may make it

105. Id. at 21–22.
106. Id. at 21.
107. Id. at 22.
109. Id.
110. Id. “One British case aptly illustrates this point. Max Mosley, a well-known figure in international racing, sued British tabloids for intrusion after they unearthed his penchant for Nazi-themed sadomasochism.” Id. “At public trial, Mr. Mosley was forced to recount the particulars and details of his fetish, as well as its effect on his health and family life.” Id. ¶ 60, at 262–63; see also John F. Burns, Trial About Privacy in Which None Remains, N.Y. TIMES, July 9, 2008, available at http://www.nytimes.com/2008/07/09/world/Europe/09mosley.html?pagewanted=1&_r=1&hp.
111. Abril & Cava, supra note 108, ¶ 61, at 263.
difficult to prosecute the suit. Finally, the Internet’s anonymity may make it difficult to identify the proper individual against whom to file suit. Nevertheless, a detailed examination of the common law doctrines as they relate to the protection of private information merits attention.

1. Tort Law

In The Right to Privacy, Samuel D. Warren and Louis Brandeis argued “for the extension of common law protection of personal privacy to nongovernmental or private party intrusion.” According to the Restatement, the common law tort doctrine addresses four privacy harms. These are intrusion, appropriation, false light and public disclosure.

In the context of electronic health records, the most relevant of the privacy harms is public disclosure; however, intrusion is also relevant.

112. Id.
113. Id. ¶ 62, at 263.

117. Intrusion is “a highly offensive invasion of another person’s seclusion or private life.” BLACK’S LAW DICTIONARY 829 (7th ed. 1999).
118. Appropriation occurs when a “person takes the name or likeness of another for commercial gain.” BLACK’S LAW DICTIONARY 98 (7th ed. 1999).
119. “In an invasion-of-privacy action,” false light is “a plaintiff’s allegation that the defendant attributed to the plaintiff views that he or she does not hold and placed the plaintiff before the public in a highly offensive and untrue manner.” BLACK’S LAW DICTIONARY 619 (7th ed. 1999).
120. Public disclosure occurs when secrets are improperly disclosed. Abril & Cava, supra note 108, at 264.
121. Id. ¶ 65, at 264.
Nevertheless, “neither tort has been successfully applied to activities occurring on online social networks.”122

In order for a claim alleging public disclosure to succeed, the disclosed information must be shameful,123 and it cannot be of public concern.124 “Courts have widely acknowledged that [p]ublic [d]isclosure only protects health information when it consists of ‘unpleasant or disgraceful or humiliating illnesses’ or ‘hidden physical or psychiatric problems.’”125 Because of this, the public disclosure doctrine is severely limited and is not a significant privacy protection.

Additionally, “courts [have] generally maintain[ed] a fairly deferential negligence standard and [they have] require[d] significant personal injury before requiring transgressors to pay victims for harm suffered.”126 Due to this, the prosecution of tort actions to recover damages for privacy torts is generally not effective since the adjudication of cases will be significantly limited if people are only minimally injured.127

2. Contract Law

One distinguishing factor that separates contract law from tort law is damages.128 Specifically, one advantage of using contract law to regulate privacy is that contract law provides claimants with injunctive relief,129 while plaintiffs using a tort-based remedy are limited to foreseeable damages.130 This is particularly useful because tort law often exacerbates the problem of

122. Id.
123. Id. ¶ 68, at 265.
124. Id. ¶ 69, at 265; see also Shulman v. Grp. W Prods., Inc., 955 P.2d 469, 497–98 (Cal. 1998) (holding that where plaintiffs were non-public figures and involved in a car accident, a television broadcast taken of their extrication from their car was of legitimate public concern). Other examples of health information deemed to be of public concern include an individual’s sterilization and a woman’s rape. Abril & Cava, supra note 108, ¶ 69, at 265; see, e.g., Bartnicki v. Vopper, 532 U.S. 514, 535 (2001); Florida Star v. B.J.F., 491 U.S. 524, 541 (1989); Howard v. Des Moines Register & Tribune Co., 283 N.W.2d 289, 304 (Iowa 1979).
125. Abril & Cava, supra note 108, ¶ 68, at 265 (citations omitted); see also Geordt v. Tribune Entm’t Co., 106 F.3d 215, 220 (7th Cir. 1997); RESTATEMENT (SECOND) OF TORTS § 652D.
127. Safier, supra note 115, at 108.
128. Abril & Cava, supra note 108, ¶ 71, at 266.
129. Id.
130. Id.
unwanted disclosure, whereas under contract law, an injunction can impede an ongoing harm. At present, the terms found in most e-commerce contracts are unregulated. This presents a problem because “[p]rivacy policies act as a warranty on the website’s use and disclosure of information,” and the enforceability of the privacy policy is dependent upon the terms of the contract.

In theory, an individual will only disclose information that is personal in exchange for a benefit, which forms a contract. While such exchanges are “quick, easy and, largely cost free” in cyberspace; there are several problems that may hinder the effectiveness of contracts to protect privacy.

First, it is difficult to obtain informed consent online. Second, “[w]ebsite contracts are built on shifting sands.” Consequently, users are faced with uncertainty as website operators can change the terms of the contracts at anytime. The FTC has even issued a report stating that, “[w]ebsites rarely provide information about when the current policies were created or updated and, if updated, exactly what changes were made. . . . They tell consumers that the policies will likely change and instruct them to check back frequently.” Finally, the enforcement mechanisms for such contracts are notoriously weak, and generally, the only recourse that users have against a website “is to seek action by the FTC or the states’ attorneys

131. See supra note 111 and accompanying text.
132. Abril & Cava, supra note 108, ¶ 71, at 266.
133. Id. ¶ 72, at 266.
134. Id.
135. Id.
136. Safier, supra note 115, at 113.
137. Id.
138. Abril & Cava, supra note 108, ¶ 73, at 266; see generally Paul M. Schwartz, Privacy and Democracy in Cyberspace, 52 VAND. L. REV. 1609 (1999). In fact, numerous surveys indicate that most users do not understand the terms used in privacy policies. HARRIS INTERACTIVE, A SURVEY OF CONSUMER PRIVACY ATTITUDES AND BEHAVIORS 6, http://www.bbbonline.org/UnderstandingPrivacy/library/harrissummary.pdf (last visited Feb. 18, 2011). This is the case because most contracts are written in a legalistic style, and since the contracts for each website visited are different, the costs associated with understanding each contract are high. Abril & Cava, supra note 108, ¶ 73, at 266–67.
139. Abril & Cava, supra note 108, ¶ 74, at 267. For example, Microsoft’s privacy statement has been modified at least three times since October 2007. Microsoft HealthVault Account Privacy Statement, supra note 58.
Thus, the answer to the problem of how to protect consumers’ privacy cannot be found in either tort law or contract law.

C. Survey of Solutions

As serious as the current medical identity theft crisis is, the widespread adoption of electronic health records will only further exacerbate the problem. This is not, however, an eventuality. Fear of identity theft, while grounded in reality, is manageable, and numerous commentators have proposed solutions to alleviate the public’s anxieties and concerns relating to the adoption of electronic health records.

Any proposed remedy must exhibit certain characteristics for it to be successful. First, the remedy must allocate risk to the party who can most efficiently bear it. The assignment of risk should encourage that party to adopt the optimal level of precaution. And finally, the remedy must be able to respond to technological changes.

While the literature is replete with proposals that aim to protect the privacy of patient health information, this Note will only focus on the two following proposals.

1. Privacy Seals

One commentator has proposed that Congress delegate to the FTC the power to issue and enforce a system of “privacy seals” modeled after the TRUSTe privacy seal system. Privacy seals modeled after the TRUSTe paradigm aim to save consumers the time and frustration “of analyzing and selecting privacy policies,” thereby allowing consumers to “limit their dealings to companies certified by privacy seal organizations.”

---

143. Id. ¶ 76, at 268.
146. Oussayef, supra note 145, at 127. Companies operating databases would “apply online at the TRUSTe website by submitting their privacy policies. If the company meets TRUSTe guidelines and its website passes a website audit and review, it can display the TRUSTe seal on its website.” Id. Furthermore, according to this commentator, the standardization plan would operate as follows:

Companies that wish to receive a privacy seal would have to select among standardized privacy policies instead of writing their own. Ideally, the FTC would...
There are nevertheless drawbacks to this proposed solution. Numerous companies who have “received the TRUSTe seal violated their privacy policy anyway[,]” and it is unlikely that the FTC will fare much better in enforcing a federal privacy seal system because the FTC’s resources are limited. And even if the FTC had the resources to prosecute every instance of privacy policy violations, the penalties that the FTC can issue are meager in comparison to the cost of medical identity theft.

While the privacy seal approach would work to ensure that service providers afford consumers a minimum level of protection, doing so may in fact further endanger consumers. This contradiction exists because the contractual promises made by service providers to consumers regarding safety do not directly correlate with the actual degree of safety experienced by consumers. Sure, companies who “guarantee” higher levels of precautions will likely invest in such precautions at higher levels. Despite this, greater investments do not necessarily lead to better protection. On occasion, the more secure website will not be the one who has guaranteed a higher level of security, but rather, has designed better security protocols and measures. Thus, consumers may be lulled into a false sense of security under a privacy seal framework because privacy seals only describe “inputs” and not results.

accept input from data brokers, advocacy groups, current privacy seal organizations, and individual consumers. It would then come up with a “menu” of policies that companies could choose from. The policies should include such factors as: (1) whether the company collects information without explicit consent, (2) whether the company retains the right to sell or exchange third party information, (3) whether the company agrees to notify all customer in case of a data breach, (4) whether the company deletes unnecessary data after a certain period of time, and (5) the company’s subpoena policy.

Id. at 128–29 (footnotes omitted).

147. Id. at 127.


149. See Robert A. Hillman, Online Boilerplate: Would Mandatory Website Disclosure of E-Standard Terms Backfire?, 104 MICH. L. REV. 837 (2006). Robert Hillman describes the legal ramifications of standardizing contractual terms in e-commerce business. He points out that “mandatory website disclosure [may] backfire and create a safe haven for businesses that are seeking to write marginal, but not outrageous terms.” Id. at 853. He also notes that “[t]erms once potentially stricken on unconscionability or related grounds might be enforceable because of their reasonable disclosure.” Id.
2. Property Rights Approach

Although the law in the United States does not generally “recognize an ownership right in mere information,” one commentator has proposed creation of such a right as a tool to protect the privacy of information. According to this commentator, the “basis for a novel privacy protection paradigm can be the recognition of a property right in one’s own health information.”

There are, however, numerous problems with such an approach. Chief among which is the problem of free alienability. It has been said that the “right of a property owner to freely transfer property rights to third parties is a fundamental aspect of property law.” This is problematic because “by granting a healthcare entity a right to use one’s propertized health information, it is assumed that the individual is also granting the healthcare entity a right to transfer the information to third parties for uses to which the individual might not have originally agreed.” What is troubling about this is that in the healthcare context, the information contained in health records is often sensitive and private in nature, and naturally, most people would not want to cede the right to control how the information contained in their records is disseminated. Because of this, it has been proposed that there should be restrictions on free alienability.

Furthermore, the “main benefit of creating a property right in one’s personal information is that it will shift bargaining power to the individual, as opposed to the information collector.” “Under a property scheme . . . the owner of a property right is able to negotiate the sale of that person’s information.” The “pre-sale negotiation pursuant to a property regime [would also allow] the individual to determine the value of the individual’s information.” Unfortunately, the value of one’s private information will be

152. Id. at 815.
153. Id.
154. Id. (citing Samuelson, supra note 150, at 1137–47).
155. Id.
156. Id. at 817.
157. Id. at 816.
158. Id. (citing Lawrence Lessig, Code Version 2.2, 279–80 (2006)).
159. Id.
difficult to quantify.\textsuperscript{160} As a result, “such a system could lead to personal information becoming under-valued and sold at too low of a price.”\textsuperscript{161} Although the author of this proposal claims that this problem could be solved by allowing “individuals to form collective organizations to determine the appropriate value of their members’ information and negotiate with information gathering entities on behalf of a large group of individuals,”\textsuperscript{162} the author does not elaborate on how such an organization would function. Nor does the author explain how individuals will be able to exert bargaining power when it has been shown with respect to contracts that the individual is usually at a disadvantage compared to the website operator for a variety of reasons.\textsuperscript{163}

Nevertheless, one of the benefits of a property regime is that it will force “businesses to internalize externalities associated with data collection as well as property rights running with the property.”\textsuperscript{164} This will in turn lead businesses to make more prudent decisions “regarding the collection and use of personal information.”\textsuperscript{165} However, it is important to note that this “may lead to a reduction in the overall amount of data being collected,”\textsuperscript{166} and this may “result in individuals receiving a pecuniary benefit in exchange for the use of their personal information.”\textsuperscript{167} What is left unexplained is how and for what purposes individuals may receive such a pecuniary benefit in exchange for the use of their information. While such a concern may seem trivial, it is nevertheless an important one considering the fact that both Google and Microsoft are offering the use of their services to consumers for free.\textsuperscript{168}

VI. A PROPOSAL TO PROMOTE THE SECURITY OF ELECTRONIC HEALTH RECORDS

Any proposed remedy must allocate risk to the party who can best bear it. This assignment of risk should also encourage that party to adopt the optimal level of precaution. And finally, the proposed remedy must be able to respond to technological changes. With this in mind, I propose that

\textsuperscript{160}\textit{Id.}
\textsuperscript{161}\textit{Id.}
\textsuperscript{162}\textit{Id.}
\textsuperscript{163}See supra notes 138–143 and accompanying text.
\textsuperscript{164}McMahon, supra note 151, at 816.
\textsuperscript{165}Id.; \textit{see also} McClurg, supra note 144, at 91–92.
\textsuperscript{166}McMahon, supra note 151, at 816–17.
\textsuperscript{167}Id. at 817.
\textsuperscript{168}See supra Part II.
Congress amend HIPAA in the following ways. First, Congress should expand the list of “covered entities” to include companies that operate databases that store electronic health records. Second, HIPAA should provide a private right of action to the victims of security breaches. And finally, HIPAA should require the companies that operate electronic health record databases to disclose information regarding security breaches publically.

At its most basic level, my proposal aims to take the best characteristics of the aforementioned proposals and doctrines while minimizing the negatives of each. For example, one of the most fundamental flaws associated with an approach based on contract law is that the terms of the contracts themselves may not provide adequate protection. When HIPAA was first enacted, health plans, healthcare clearinghouses, and healthcare providers were essentially the only entities that regularly transmitted health information electronically. This, however, is no longer the case, and because of this, regulations that once safeguarded patient health information now leave consumers vulnerable because their health information is only as secure as the least secure entity to possess the information. Therefore, Congress should expand HIPAA’s list of “covered entities” to include electronic health records service providers, and by doing so, companies that operate electronic health records systems would be required to comply with the national standards for electronic healthcare transactions set by the Department of Health and Human Services, thereby extending to consumers a minimum floor of protection. Another factor hindering the use of common law doctrines is that not all jurisdictions accept these doctrines. Therefore, the creation of a private right of action will aid consumers in those jurisdictions by providing them with a means to seek redress. Finally, the creation of a public disclosure requirement will help mitigate the crisis by providing consumers with the information necessary for them to make informed decisions regarding which company’s services they will utilize, and this will provide companies with the incentive to invest in precautions to safeguard patient health information. Thus, my proposal will provide consumers with both a remedy for any damages that they have suffered because of improper disclosures, and it will provide incentives for service providers to prevent those improper disclosures in the first place.

169. See generally supra Part V.
170. See supra Part III.
171. See supra Part III.
A. Congress Should Expand the List of “Covered Entities”

Since HIPAA’s regulations only apply to “covered entities,” consumers who utilize the services of companies such as Google and Microsoft are limited to the protections afforded to them under their user agreements and the Federal Trade Commission Act.\footnote{172}{Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (2006).}

Under the Federal Trade Commission Act, the FTC is “empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce . . . .”\footnote{173}{15 U.S.C. § 45(a)(2) (2006).} The Commission has the power to issue orders “requiring such person, partnership or corporation to cease and desist” from using such unfair methods of competition or deceptive practices.\footnote{174}{15 U.S.C. § 45(b) (2006).} And when a person, partnership or corporation violates such an order “after it has become final, and while [it is] in effect,” that person or entity must “pay to the United States a civil penalty of not more than $10,000 for each violation . . . .”\footnote{175}{15 U.S.C. §45(l) (2006).}

Google even references these provisions on its website, stating that the Federal Trade Commission Act “enforces privacy protections in the Google Health privacy policy through civil and criminal penalties.”\footnote{176}{Google Health and HIPAA, supra note 47.} Nevertheless, consumers should not simply rely on the Federal Trade Commission Act, because the Federal Trade Commission Act merely enforces end user agreements between consumers and companies, and while this may be sufficient when the end user agreement provides ample protections,\footnote{177}{See generally supra Part II.A.2.} not all companies provide such protections in their user agreements, thereby shifting the costs of security breaches to the consumer. To rectify this deficiency, the list of “covered entities” should be expanded to include companies such as Google and Microsoft, thereby affording consumers with a minimal floor of protections that the Department of Health and Human Services will establish.\footnote{178}{Although Google Health and Microsoft HealthVault are similar in many respects, this Note presented both in Part II.A because Google and Microsoft provide users with different privacy protections. For example, Google allows users to revoke third-party access to their records at any time, see supra notes 39–46 and accompanying text, while Microsoft HealthVault allows a user to grant custodian access to a third party who may then revoke the original user’s access to their own record, see supra notes 60–68 and accompanying text.}
B. Private Right of Action

While the HIPAA Security Rule provides for both civil and criminal penalties against individuals who knowingly and wrongfully disclose personally identifiable information,\textsuperscript{179} and against covered entities for disclosures of protected information,\textsuperscript{180} the Secretary of Health and Human Services “can only fine covered entities a maximum of $100 per violation, and not more than $25,000 per year for multiple identical violations.”\textsuperscript{181}

Clearly then, covered entities are not required to bear the costs of data breaches when they occur, since any large scale data breach has the potential to generate more than $25,000 in damages. Because of this, covered entities do not have the incentive to invest in the proper level of precautions. Therefore, it is necessary to provide consumers with a private right of action, thereby nullifying the debate on whether the courts should extend common law tort and contract doctrines to the internet. Furthermore, the maximum fines should be significantly increased to reflect the damages actually borne by victims of data breaches. By doing this, not only will consumers have a right of action whereby they can attempt to recover for the damages that they have sustained, but the companies operating electronic health record databases will better bear the costs of data breaches and this will act as an incentive for them to invest in precautions.

C. Public Disclosure Requirement

Providing consumers with information concerning the actual security of their information will enable them to make better choices regarding where to store it. When e-commerce first emerged in the late 1990s, many consumers were reluctant to shop online,\textsuperscript{182} and while the reasons for this phenomenon were numerous, they bear on the development of electronic health records.

\textsuperscript{181}. McMahon, supra note 151, at 803; see also 45 C.F.R. §160.404 (2007).
\textsuperscript{182}. “From being almost a novelty in 1995, online retailing sales were expected to reach $7 billion by 2000. . . . Internet stores allow consumers to shop from the convenience of remote locations. Yet most of these Internet stores [lost] money.” Amit Bhatnagar, Sanjog Misra & H. Raghav Rao, \textit{On Risk, Convenience, and Internet Shopping Behavior}, 43 \textit{COMM. OF THE ACM}, Nov. 2000, at 98, 98 (footnotes omitted).
There are numerous explanations for why consumers were originally hesitant to shop online. Many were “concerned about the security of transmitting credit card information over the Internet,” and some were “apprehensive about buying something without touching or feeling it and being unable to return it if it fails to meet their approval.” Due to this, one commentator has argued that “the most significant long-term barrier for realizing the potential of Internet marketing to consumers will be the lack of consumer trust, both in the merchant’s honesty and in the merchant’s competence to fill Internet orders.”

Hence, “trust” serves as the foundation for all commercial relationships. It is especially important as “a governance mechanism in exchange relationships that are characterized by uncertainty, vulnerability, and dependence.” However, “[t]rust is a critical factor in any relationship in which the trustor (e.g., consumer) does not have direct control over the actions of a trustee (e.g., merchant or store), the decision is important, and the environment is uncertain.”

Therefore, the success of electronic health records will largely depend upon whether consumers trust the companies and institutions responsible for the implementation and control of those records, as consumers do “not have direct control over the actions” of companies that operate electronic health records databases. What’s more, the decision to upload one’s health records to an online database can have far-reaching consequences, and like the e-commerce environment, the environment for electronic health records is fraught with uncertainty.

What is necessary therefore is a solution that fosters trust between consumers and the companies that operate electronic health care databases. However, trust should not be encouraged artificially. Rather, consumers should be encouraged to trust only those companies whose past performance indicates that their patron’s health information will be secure in the future.

183. Id.
184. Id.
186. Id.
187. Id. at 46.
188. Id. at 45.
189. Id. However, it is worth mentioning that both Google and Microsoft provide their consumers with significant control over their records. See generally supra Part II.A.2.
190. See supra Part IV.B.
191. See supra Part IV.B.
Congress can facilitate this by amending HIPAA to require all companies to disclose information regarding security breaches publicly.\textsuperscript{192} By doing this, consumers will be able to judge the efficacy of the security procedures implemented by companies operating electronic health record systems, and consumers will consequently be able to make informed decisions as to which company’s services they should procure. Providing consumers with this capability will then give companies the incentive to improve their security protocols and procedures,\textsuperscript{193} because consumers will

\begin{footnotesize}
\textsuperscript{192} For a thorough discussion of public disclosure requirements, see Brendan St. Amant, \textit{The Misplaced Role of Identity Theft in Triggering Public Notice of Database Breaches}, 44 HARV. J. ON LEGIS. 505 (2007). Supporters of linking the consumer notification trigger to the risk of identity theft make the valid point that a more sensitive trigger could lead to over-notification. They further argue that over-notification may desensitize victims (causing them to ignore all threats), or may lead to needless business expenditures undertaken to placate consumers who seek unnecessary card and account replacements in response to false alarms.

But this presumes that the total costs associated with these outlays from over-notification [sic] exceed the potential pitfalls of undernotification [sic]. While a lower threshold for notification may result in some short-term losses, these costs could be addressed through higher fees for consumers. Whether these increases are significant enough to outweigh their ability to mitigate the extent of overall loss achieved by warning victims is an empirical question. An increase in mass notification also signals to potential identity thieves that the information is being monitored, and reduces the expected benefits from theft, potentially prompting some to refrain from committing the crime.

A preferable provision for triggering notification, which should deter fraud and better account for non-pecuniary risks, would state that notification of security breaches is required unless there is no risk of harm. Determining whether or not a risk of harm exists for these purposes would, again, be a product of the consultation between state or federal authorities and would occur before a business could proceed to notify the public at large.\textit{Id.} at 524–25 (footnotes omitted).

\textsuperscript{193} See generally Dennis D. Hirsch, \textit{Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law}, 41 GA. L. REV. 1 (2006). In \textit{Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law}, Dennis Hirsch describes two generations of thought on environmental regulations and applies the lessons learned from environmental regulations to privacy regulations. \textit{Id.} at 4–11. According to Hirsch, first generation environmental regulations were based on a “command-and-control” structure. \textit{Id.} at 33. This “method begins with government officials designating the industry that must curtail its emissions.” \textit{Id.} “Next, regulators identify the best currently existing technology for controlling pollution in that industry (known as the ‘reference technology’).” \textit{Id.} “Finally, government officials either direct all facilities in the industry to install the chosen technology . . . or require that they not exceed the rate of pollution that they would emit if they
naturally patronize the services of only those companies who have exemplary service records.\footnote{194}

Obviously, the success of this requirement depends upon how companies present negative statistics, because companies who have improperly released patient health data will naturally want to minimize negative information. In fact, companies often employ extensive public relations strategies to minimize public awareness of security breaches.\footnote{195} Therefore, the format of these disclosures should be standardized, and to do this, Congress should loosely model this amendment to HIPAA on the aforementioned privacy seal

had installed the reference technology. . . .” \textit{Id.} (footnote and emphasis omitted). Second-generation policies, on the other hand, “are those that encourage facilities to come up with their own cost-effective approaches to achieving environmental goals and that allow these self-directed actions to count towards regulatory compliance.” \textit{Id.} at 38 (emphasis omitted). In 1995, Congress’s Office of Technology and Assessment published a report stating that second-generation policies were superior to first generation ones. \textit{Id.} at 37. “The Report concluded that ‘those instruments that shift responsibility for determining the means and timing of compliance to individual firms or groups of firms’ are likely to generate far more cost-effective responses to environmental problems.” \textit{Id.} (quoting \textit{Office of Tech. Assessment}, U.S. \textit{Congress, Environmental Policy Tools: A User’s Guide} 24 (1995), \textit{available at} http://www.princeton.edu/~ota/disk1/1995/95179517.pdf). The Report further found that “[s]econd generation strategies also tend to do a better job of promoting new and better approaches to pollution reduction.” \textit{Id.} at 38 (citing \textit{Office of Tech. Assessment, supra} at 37).

\footnote{194} Dennis Hirsch further describes a strategy for privacy protection based on a second-generation environmental strategy known as the “Pollution Release and Transfer Registers.” \textit{Id.} at 57–58. One such register—the “Emergency Planning and Community Right to Know Act (EPCRA)”—required “companies to annually . . . report the quantity of hazardous chemicals that they have released into the environment or transferred off-site.” \textit{Id.} at 57; \textit{see also} 42 U.S.C. § 11023(f)(1)(A)–(B) (2000) (defining toxic chemical threshold amounts); \textit{Stephen Johnson, Economics, Equity, and the Environment} 197 (2004) (explaining the EPCRA as “[o]ne of the most effective and best known information disclosure laws”). The publication of this information provided a “strong incentive for businesses to reduce their toxic releases,” and a study of toxic releases from 1988 to 1998 indicated that toxic releases decreased by 45.3% during that time-period, thereby confirming the theory that disclosure provides an incentive for companies to modify their practices. Hirsh, \textit{supra} note 193, at 57–58. Additionally, Dennis Hirsh postulates that the incentives for “digital” companies are greater compared to industrial companies, since “[i]ndividuals often cannot choose which producers of industrial chemicals they will patronize. Yet they make direct choices about which credit cards they hold, where they bank, and which e-commerce sites they visit.” \textit{Id.} at 58.

\footnote{195} For example, in 2005 Choice Point suffered a security breach. St. Amant, \textit{supra} note 192, at 508 (citing David Lazarus, \textit{Shifting Sands in Data Leak}, S.F. \textit{Chron}, Feb. 25, 2005, at C1). Three months later, ChoicePoint first began notifying its consumers and it framed the security breach as “‘crimes committed against ChoicePoint’ and ‘fraud against the company.’” \textit{Id.} at 516 (quoting Lazarus, \textit{supra}, at C1).
proposal. Consequently, as a part of this amendment to HIPAA, Congress should delegate to the Department of Health and Human Services the power to create and enforce guidelines governing how companies present adverse information, which should regulate the timing, format and the content of disclosures.

The timing of disclosures is especially relevant in the context of medical identity theft for two reasons. First, the disclosure of a data breach will enable consumers to take remedial action to protect their identities after a data breach. Second, timely disclosure will allow consumers to make informed decisions when they are contemplating whether to patronize the services of a particular company.

Moreover, the aforementioned TRUSTe proposal demonstrates why it is necessary to regulate the format and content of disclosures. By standardizing the format and content of disclosure requirements, consumers, the government, and the courts will become accustomed to the disclosures, and precedents will develop regarding what is required in a disclosure.

196. According to U.S. News & World Report, victims of medical identity theft should take the following remedial actions:

[1] Get a copy of your medical records from healthcare providers and review them to make sure they’re consistent with treatment you’ve received. [2] Ask your insurer for copies of all “Explanation of Benefits” statements for the past year. . . . Review these for accuracy, too. [3] Get a free copy of your credit report from one of the three credit bureaus. . . . Sometimes collection notices for unpaid bills alert victims to theft. [4] File a police report if you’re a victim. It may encourage providers and your insurer to correct your records promptly.


197. See supra notes 145–149 and accompanying text.


199. Id. With respect to privacy policies, standardization will deter companies from intentionally violating their privacy policies. Since the FTC will be very familiar with the limited number of privacy policies, it will be easier to detect violations. Companies will also have less leeway to use their vague language to escape responsibility. Courts can develop precedent as what constitutes a breach of particular policies, further increasing predictability. Additionally, the FTC could require that companies who violate their policy be placed on probation. Probation might be represented by “negative seal” that would warn consumers of a recent data breach. These factors would serve as a powerful deterrent against intentionally violating privacy policies.

Id. at 130. Although different, one could easily see how the effects of standardization on privacy policies will be similar to its effect on the same with disclosure requirements.
In the future, as electronic health records replace traditional paper records, those electronic health records will become vulnerable in ways presently unimaginable.200 This is precisely why I proposed a dynamic solution, in this Note, to the medical identity theft crisis. By amending HIPAA to include those companies that operate electronic health records systems,201 Congress would empower the Department of Health and Human Services to establish national standards for such systems;202 thereby enabling the Department of Health and Human Services to promulgate or amend those national standards as the threats to the security of electronic health records evolve. The creation of a private right of action203 would also not only provide the victims of data breaches with a means to recover for the damages that they have sustained, but it would, in conjunction with the public disclosure requirement,204 provide an incentive for the companies that operate electronic health records systems to invest in the proper level of precautions, which will vary as the threats to those systems develop. Thus, the enactment of this Note’s proposal will create a multi-faceted framework designed to protect electronic health records from the threats as they exist today, and as they will exist in the future, and in so doing, this proposal will, if enacted, encourage the development and adoption of electronic health records.

201. See supra Part VI.A.
202. See SULLIVAN, supra note 71, at xiii (explaining that Title II of HIPAA allows the Department of Health and Human Services to create standards for electronic health care transactions).
203. See supra Part VI.B.
204. See supra Part VI.C.