THE FUTURE OF PRIVACY IN A UNIFIED NATIONAL HEALTH INFORMATION INFRASTRUCTURE

Dennis J. McMahon[*]

I. INTRODUCTION

Since the early 1990s, the federal government has set its sights on enacting legislation to establish a national infrastructure for the storage and transmission of electronic health records.[1] In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) to protect individuals from abuse by health insurance companies and to provide a "floor" of mandatory privacy standards for certain healthcare entities.[2] HIPAA, as well as other federal privacy protections, however, has become antiquated and inadequate.[3] Thus, members of Congress are currently considering an array of bills intended to regulate the use of medical information by the healthcare industry.[4]

The federal government's current approach to increasing efficiency in healthcare, while lowering its cost by creating a national electronic health information infrastructure, will significantly impact personal privacy and the ability to secure such information.[5] It is imperative, therefore, that this legislation include provisions that safeguard personal privacy and protect confidential information from potential third-party abuse.

[*] J.D. candidate, 2008, Seton Hall University School of Law; B.S.M.E., 2005, Villanova University.

[1] *See* United States Health Service Act, H.R. 2061, 103d Cong. (1993) (establishing a United States Health Service to coordinate state and local healthcare entities); H.R. 1534, 102d Cong. (1991) (requiring the Secretary of Health and Human Services to study national healthcare systems of other developed countries and to make recommendations for legislation based on its findings to improve healthcare in the U.S.); National Health Care and Cost Containment Act, H.R. 2530, 102d Cong. (1991) (granting financial and other incentives to assist and encourage creation of a universal healthcare system).

[2] *See infra* Part II.E.

[3] *See infra* Part II.B–E.

[4] *See infra* Part III.

[5] *Id.*

Along with the benefits of a unified, national healthcare infrastructure come the problems associated with increased access to health records and electronically stored information.[6] That various institutions have incentives to misappropriate medical information augments the need for a solution.[7] There are, however, several methods of privacy protection available to eliminate, or at least mitigate, the negative effects on information privacy and security that a national healthcare infrastructure will engender.[8]

This Comment begins with an overview of the current state of healthcare privacy law and the need for adequate privacy protection. Part III then describes and analyzes selected bills which are paradigmatic of the various approaches that Congress currently contemplates. Part IV examines different methods of privacy protection available to supplement these bills. Part IV also argues that the most effective way to protect personal privacy in a national health information infrastructure is through a multi-layered approach which utilizes a new property right in personal information along with contractual and tort-based protection.

II. BACKGROUND

A. A Need for Privacy

As health information has become increasingly computerized, the risks associated with misappropriation are heightened. The electronic storage and transmission of health information creates opportunities for such information to be accidentally or intentionally disclosed to the wrong people.[9] Moreover, the consequences of misappropriation are especially severe within the realm of health-related information.[10]

Transmission of health information through the Internet allows "information to be transmitted anywhere in the world quickly,

---

[6] *See infra* Part II.A.

[7] *Id.*

[8] *See infra* Part IV.

[9] Sonia W. Nath, *Relief for the E-Patient? Legislative and Judicial Remedies to Fill HIPAA's Privacy Gaps*, 74 GEO. WASH. L. REV. 529, 530 (2006).

[10] Protection of health records is especially important because of the personal nature of the information they contain as well as the importance of health record integrity. *See Errors Across the Internet*, CONSUMER REPORTS.ORG, Mar. 2006, http://www.consumerreports.org/cro/health-fitness/health-care/electronic-medical-records-306/errors-across-the-internet/index.htm; *Safeguarding Against Theft*, CONSUMERREPORTS.ORG, Mar. 2006, http://www.consumerreports.org/cro/health-fitness/health-care/electronic-medical-records-306/safeguarding-against-theft/index.htm.

cheaply, and with relatively little risk of detection."[11] Moreover, electronic health records have the ability to contain vast amounts of sensitive information.[12] Additionally, it can be difficult to permanently delete information from a hard drive, leaving many files available for misappropriation, despite a healthcare entity's best efforts to destroy personal information.[13] Many computer programs store information in hidden files, which can contain large amounts of confidential information and can be misappropriated.[14] There are also risks associated with employees' authorized access to such information. Some privacy experts believe that the most critical risks to healthcare information are disgruntled employees and social engineering.[15] Further, when electronic data is divulged online, it is difficult to remove and becomes available to anyone.[16] Individuals that have been harmed by such disclosure may have little recourse, since it can be difficult to ascertain which party is responsible for the disclosure.[17]

There have been too many examples of health information privacy being compromised over the last few years. In 2001, a security breach caused Eli Lilly & Co. to distribute emails containing the email addresses of 699 users of Prozac, an anti-depressant manufactured by the company.[18] In 2005, approximately ten million records were reported missing between February and June alone.[19] In Janu-

[11] Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 332 (2007).

[12] Mitchelle C. Pierre, *New Technology, Old Issues: The All-Digital Hospital and Medical Information Privacy*, 56 RUTGERS L. REV. 541, 547 (2004) ("Patient medical records have come to include more sensitive information such as HIV status, psychiatric records, lifestyle details, and genetic information.").

[13] *See* John R. Mallery, *Secure File Deletion: Fact or Fiction?*, SANS INSTITUTE, July 16, 2001, http://www.sans.org/reading_room/whitepapers/incident/631.php?portal=5e905d2d4abce38f2e1de8f3f10812c6.

[14] *Id.*

[15] *See* Malcom Allen, *Social Engineering: A Means to Violate a Computer System*, SANS INSTITUTE, June 2006, http://www.sans.org/reading_room/whitepapers/engineering/529.php?portal=4b978ba268574768302191032cc4a58f. Social engineering has been defined as "[a] euphemism for non-technical or low-technology means—such as lies, impersonation, tricks, bribes, blackmail, and threats—used to attack information systems." *Id.* at 4.

[16] Hoffman & Podgurski, *supra* note 11, at 335.

[17] *Id.*

[18] News Release, Federal Trade Comm'n, Eli Lilly Settles FTC Charges Concerning Security Breach, (Jan. 18, 2002), *available at* http://www.ftc.gov/opa/2002/01/elililly.htm.

[19] Hoffman & Podgurski, *supra* note 11, at 332.

ary 2006, hackers gained access to a Notre Dame database.[20] In April 2006, a man was arrested for hacking into a University of Southern California database and accessing the records of over 270,000 applicants.[21] In May 2006, hackers misappropriated the health and financial information of 200,000 individuals from an Ohio University database.[22] Many pharmaceutical companies do not "review[] the effectiveness of their security policies and procedures" and only eighty-two percent of pharmaceutical companies reported feeling confident in their ability to protect private information.[23] Further, according to one survey, eighty-four percent of all large businesses in the United Kingdom experienced premeditated and malicious security breaches in 2006.[24]

Arguably, however, the most severe threats to health information privacy come from private business entities. Personal health information may be used by employers to hire only healthy employees and thereby reduce insurance costs; by banks to ensure repayment of loans; by drug companies seeking to target individuals and doctors for marketing products; and by health insurance companies for setting insurance premiums.[25] Correspondingly, studies have shown that between thirty-five and fifty percent of America's largest companies use personal health records to make employment decisions.[26] Consequently, the data mining and warehousing industry has flourished since the early 1990s, amassing astronomically vast amounts of

[20] Greg Sandoval, *Notre Dame Probes Hack of Computer System*, CNETNEWS.COM, Jan. 23, 2006, http://news.com.com/Notre+Dame+probes+hack+of+computer+system/2100-1029_3-6030229.html?tag=st.rn.

[21] Stefanie Olsen, *Man Charged with Hacking USC Database*, CNETNEWS.COM, Apr. 20, 2006, http://news.com.com/Man+charged+with+hacking+USC+database/2100-7350_3-6063470.html?tag=st.rn.

[22] Greg Sandoval, *Ohio University Suffers Security Breaches*, CNETNEWS.COM, May 11, 2006, http://news.com.com/2100-7349_3-6071505.html.

[23] PRICE WATERHOUSE COOPERS, THE 2004 GLOBAL INFORMATION SECURITY SURVEY (2005) available at http://www.biznespolska.pl/files/reports/Pharma%20Alert_Dec%202004%20_Security%20Survey_v7.pdf.

[24] PRICE WATERHOUSE COOPERS DEPARTMENT OF TRADE AND INDUSTRY, INFORMATION SECURITY BREACHES SURVEY 2006 (2006) *available at* http://www.pwc.com/uk/eng/ins-sol/publ/pwc_dti-fullsurveyresults_execsum06.pdf.

[25] Hoffman & Podgurski, *supra* note 11, at 334.

[26] *See Testimony Before the Subcomm. on Gov't. Mgmt., Info., & Tech. of the H. Comm. on Gov't. Reform & Oversight*, 105th Cong. (1998) (statement of Janlori Goldman, Director, Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University) (stating that thirty-five percent of Fortune 500 companies use health information in employment decisions); *see also* ROSS J. ANDERSON, SECURITY IN CLINICAL INFORMATION SYSTEMS 5 (British Medical Association) (1996) *available at* http://www.cl.cam.ac.uk/~rja14/Papers/policy11.pdf.

personal information.[27] Currently, over one thousand data mining and warehousing companies are collecting the personal information of American consumers.[28] Moreover, these companies keep information on virtually every household; some claiming to have amassed over one thousand pieces of data on the average household.[29] Similarly, a company known as the Medical Information Bureau (MIB) amasses personal health information about almost everyone obtaining, or attempting to obtain, health insurance.[30] Insurance companies typically gather this information when an individual applies for health insurance and then report it to the MIB in a series of codes.[31] Although the MIB keeps its list of codes secret, researchers claim that the MIB uses hundreds of codes to describe information including AIDS, diabetes, heart problems, drug use, smoking, adverse driving records, hazardous sports, sexual deviance, and sloppy appearance.[32] Subsequently, when an individual applies for insurance with another insurance company, this information is used to deny coverage or to raise premiums.[33] Unfortunately, HIPAA does not protect this information because the MIB codes are not considered protected health information.[34]

Increased consumer awareness of the potential harm caused by misuse of personal information has led to inefficiency in healthcare. Physicians depend on patients to provide truthful and complete information.[35] As one commentator noted, "[i]f patients have concerns about the privacy of their health information, they are less likely to divulge pertinent information for fear of inappropriate disclosures, which could result in inappropriate or incorrect treatment."[36] In fact, a recent National Consumer Health Privacy survey showed that sixty-seven percent of the population is "somewhat" to "very" concerned

[27] Tal Z. Zarsky, *"Mine Your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, 5 YALE J.L. & TECH. 1, 2 (2003).

[28] Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 65 (2003).

[29] *Id.* at 65–66.

[30] *See* Simson Garfinkel, *Nobody Knows the MIB*, *in* INFORMATION PRIVACY LAW 348–50 (2006).

[31] *See id.*; s*ee also* Privacy Rights Clearinghouse, Fact Sheet 8: Medical Records Privacy, http://www.privacyrights.org/fs/fs8-med.htm#C (last visited Oct. 22, 2007).

[32] *See* Garfinkel, *supra* note 30, at 349.

[33] *See id.*

[34] *See* Privacy Rights Clearinghouse, *supra* note 31. The MIB, however, is a consumer reporting agency under the Fair Credit Reporting Act. *Id.*

[35] Nath, *supra* note 9, at 530–31.

[36] *Id.* at 531.

about medical record confidentiality.[37] Additionally, thirteen percent admitted to avoiding disclosure to medical practitioners in some way to protect their information.[38] Similarly, a study by the American Health Information Management Association showed that thirty percent of healthcare providers reported an increase in patients who ask questions about privacy concerns, while twenty-two percent have reported an increase in the number of patients who refuse to sign release of information forms.[39] Therefore, the current lack of adequate privacy protection frustrates the goal of increasing the quality of healthcare.[40] Creating a national health information infrastructure will only augment the loss of privacy associated with the increase in health information technology.[41]

B. Constitutional Protection

The Bill of Rights provided the earliest and most basic privacy protection for American citizens.[42] Although the Framers of the Constitution arguably could not have envisioned the stark increase in technology—along with the increase in the complexity of daily life which has given rise to a need for information privacy protection—the Supreme Court of the United States has interpreted the Constitution to include a right of privacy in one's personal information.[43] As applied to private health information, however, the right has a very narrow scope and is limited to provide inadequate privacy protection for confidential medical information.[44]

The Supreme Court first articulated a fundamental right to privacy in *Union Pacific Railway v. Botsford*.[45] There, the Court held that a

---

[37] Hoffman & Podgurski, *supra* note 11, at 335 (citing LYNNE BISHOP ET AL., CALIFORNIA HEALTH CARE FOUNDATION, NATIONAL CONSUMER HEALTH PRIVACY SURVEY 2005: EXECUTIVE SUMMARY 3 (2005)).

[38] *Id.* ("Furthermore, thirteen percent of respondents claimed that they had attempted to protect their own privacy by avoiding medical tests or visits to their regular physicians, asking doctors to distort diagnoses, or paying for tests out-of-pocket so that no medical documentation would be sent to insurance companies.").

[39] AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION, THE STATE OF HIPAA PRIVACY AND SECURITY COMPLIANCE 12–14 (April 2006).

[40] Nath, *supra* note 9, at 531.

[41] *See* Pierre, *supra* note 12, at 547–48.

[42] *See* U.S. CONST. amends. I, III, IV, V, IX; *see also* Griswold v. Connecticut, 381 U.S. 479 (1965).

[43] Whalen v. Roe, 429 U.S. 589, 598–602 nn.23–24 (1977). Although the Court held that there was no constitutional privacy violation in the statute, it provided examples of different types of constitutional privacy protection for information and explained that the scope of privacy protection is unclear. *Id.*

[44] *See infra* notes 52–69 and accompanying text.

[45] 141 U.S. 250 (1891).

plaintiff could not be compelled to undergo a surgical examination in a civil action.[46] The Court described a "sacred" right of privacy that must be "carefully guarded."[47] Moreover, in *Griswold v. Connecticut*,[48] the Supreme Court interpreted the First, Third, Fourth, Fifth, and Ninth Amendments as incidents of the Bill of Rights protecting a greater, fundamental concept of a right to privacy.[49] Subsequently, the Court considerably expanded this right when it applied the fundamental right to privacy under various circumstances.[50] Beginning in the late 1970s, however, a judicial trend emerged to limit the scope of constitutional privacy protection specifically pertaining to medical information.[51]

Whalen v. Roe[52] was the first major case limiting constitutional protection for private medical information.[53] *Whalen* involved a controversial New York law which required detailed information regarding patients who received Schedule II prescription drugs[54] to be stored in a government database.[55] The Court identified two categories of personal privacy violations: "disclosure of personal matters" and preventing "independence in making certain kinds of important decisions."[56] Further, the Court acknowledged the danger and negative consequences associated with maintaining a database of confidential medical records.[57] Nevertheless, the Court determined that the threat posed by the law did not meet the threshold of severity necessary to be violative of the Constitution.[58] Thus, the scope of

[46] *Id.* at 255.

[47] *Id.* at 251.

[48] 381 U.S. 479 (1965).

[49] *Id.* at 484–85.

[50] *See, e.g.*, Lawrence v. Texas, 539 U.S. 558 (2003) (invalidating a state law prohibiting sodomy between same-sex couples); Roe v. Wade, 410 U.S. 113 (1973) (holding a state law prohibiting abortion invalid for interfering with a constitutional right to privacy); Eisenstadt v. Baird, 405 U.S. 438 (1972) (expanding the fundamental right to privacy in the use of contraceptive devices found in *Griswold v. Connecticut* to protect non-married individuals).

[51] *See* Whalen v. Roe, 429 U.S. 589, 603–07 (1977).

[52] 429 U.S. 589 (1977).

[53] *Id.* at 598–605.

[54] New York State law classifies the most dangerous prescription drugs as Schedule II prescription drugs. *Id.* at 593 & n.8. These drugs have legitimate medical purposes but are highly likely to be abused. *Id.*

[55] *Id.* at 593.

[56] *Id.* at 598–600.

[57] *Id.* at 604–07.

[58] *Whalen*, 429 U.S. at 603–04. Although the Court did not explicitly state the level of severity needed to implicate a violation of constitutional privacy protection, it noted that "neither the immediate nor the threatened impact . . . on either the reputation or the independence of patients . . . is sufficient to constitute an invasion of

constitutional protection for medical information privacy was unclear after *Whalen*. Although the Court did not eliminate the possibility that a constitutional cause of action would lie, it set a high threshold for success on such a claim.[59]

In *Doe v. Southeastern Pennsylvania Transportation Authority*,[60] the U.S. Court of Appeals for the Third Circuit, confronting what many would consider an egregious misappropriation and disclosure of personal information,[61] further restricted the role of the Constitution in protecting health information privacy.[62] In that case, a state employer discovered an employee's status as an AIDS patient by viewing prescription drug records provided pursuant to a health insurance agreement.[63] Thereafter, the employer disclosed this information to other employees.[64] The plaintiff, known as Doe, consequently sued the employer, alleging that the employer violated his constitutional right to privacy under the Fourteenth Amendment.[65] The court used a seven-factor test, first articulated in *United States v. Westinghouse Electric Corp.*,[66] to determine whether the interest in reducing the cost of health insurance and preventing fraud outweighed the invasion of Doe's personal privacy.[67] Moreover, the court noted that the distinguishing factor between this case and prior cases, in which the privacy

any right or liberty protected by the Fourteenth Amendment." *Id.* Concurring, Justice Brennan stated that the "interest in avoiding disclosure of personal matters" is not "seriously enough invaded" in this case because the State limited the number of people with access to this information and put restrictions on disclosure. *Id.* at 606 (Brennan, J., concurring). However, Justice Brennan noted that new computer technology "vastly increase[s] the potential for abuse of that information," and that in the future there may be a need to "curb . . . such technology." *Id.* at 607.

[59] *See id.* at 603–07 (majority opinion).

[60] 72 F.3d 1133 (3d Cir. 1995).

[61] *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1438–39 (2001).

[62] *Doe*, 72 F.3d 1133.

[63] *Id.* at 1135–36.

[64] *Id.*

[65] *Id.* at 1137–38.

[66] 638 F.2d 570, 578 (3d Cir. 1980).

[67] *Doe*, 72 F.3d at 1140 (citing *Westinghouse*, 638 F.2d at 578).

> *Westinghouse* mandates a consideration of seven different factors. They are: (1) the type of record requested; (2) the information it does or might contain; (3) the potential for harm in any subsequent nonconsensual disclosure; (4) the injury from disclosure to the relationship in which the record was generated; (5) the adequacy of safeguards to prevent unauthorized disclosure; (6) the degree of need for access; and (7) whether there is an express statutory mandate, articulated public policy, or other recognizable public interest favoring access.

Id.

interest prevailed, was the lack of harm caused by collecting and using Doe's data.[68] However, this decision ignores serious intangible and psychological harm in favor of a mild state interest.[69]

In the wake of these cases, it is apparent that constitutional privacy protection is too limited to adequately handle the privacy risks associated with a unified national health information infrastructure. First, the courts have failed to conceptualize the potential scope of the harm caused by breaches of privacy in health information.[70] The court in *Doe* did not understand that "[Doe's] real injury was the powerlessness of having no idea who else knew he had HIV, what his employer thought of him, or how the information could be used against him. . . . [T]he information appeared to be entirely out of anyone's control."[71] Second, the courts have not accurately realized the range of security risks posed by electronic storage of health information. This is evident from the *Whalen* Court's pronouncement that disclosure of medical information can occur in only three ways: through(1) either deliberate or negligent employee action, (2) evidence in a judicial proceeding, or (3) voluntary disclosure.[72] Obviously, in a national infrastructure of databases that transmits information electronically to doctors, insurance companies, patients, and other medical staff, there are many ways in which personal data may be misappropriated. The failure to grasp both the nature of the harm caused by a breach of privacy and the methods by which data can be misappropriated has caused lower courts to adopt tests for constitutional privacy violations that reduce the weight given to privacy concerns in favor of marginally legitimate state interests in obtaining information.[73]

C. State and Common Law Information Privacy Protection

State and common law privacy protection is inadequate because, in addition to varying between states, it tends to focus on physician-patient confidentiality, which can only cover a small portion of the

[68] *Doe*, 72 F.3d at 1140–43.

[69] *See* Solove, *supra* note 61, at 1438.

[70] *See id.*

[71] *Id.* at 1438–39.

[72] *See* Whalen v. Roe, 429 U.S. 589, 600 (1977). Although the Court was specifically addressing privacy concerns regarding the New York statute at issue in this case, the Court stated generally that "[p]ublic disclosure of patient information can come about in three ways." *Id.*

[73] Pierre, *supra* note 12, at 564.

threats to data in a national health information infrastructure.[74] Since actions which allege breaches of confidentiality are typically only successful if they also allege a fiduciary relationship between a doctor and a patient, such actions cannot be brought against many third-party practitioners or entities who interact with or maintain patient information.[75] Yet these entities are equally capable of divulging private medical information and can be entirely out of the reach of traditional tort law. As one commentator points out, because the health record itself contains information collected by several primary and secondary sources, "[f]ocusing legal protection on a single therapeutic relationship within this information environment is an anachronistic vestige of an earlier and simpler time in medicine."[76] Thus, the current scheme of common law tort protection will not satiate the need for adequate privacy protection in a national healthcare information infrastructure.[77]

D. The Privacy Act of 1974

Congress passed the Privacy Act of 1974 ("Privacy Act") in response to growing public concern over government agencies using electronic means to amass large databases that contain personal information.[78] The Privacy Act aimed to abate these concerns by allowing individuals to access and control records stored by the federal government and by limiting the government's ability to use and disclose private information.[79] This attempt at omnibus legislation, which requires government compliance with fair information practices, is incapable of sufficiently protecting individuals' health information in a national healthcare information infrastructure.[80]

---

[74] *See* JOY PRITTS ET AL., THE STATE OF HEALTH PRIVACY (Georgetown University 2d ed. 2002) (1999) (surveying and comparing various state privacy laws) *available at* http://medicalrecordrights.georgetown.edu/pdfs/statereport1.pdf; *see also* Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 511–12 (1995).

[75] Gostin, *supra* note 74, at 512. Third-party practitioners and entities could include nurses, medical testing facilities, medical testing technicians, or other agents and employees of a healthcare entity who do not interact directly with the patient. *Id.*

[76] *Id.*

[77] Lawrence O. Gostin et al., *The Nationalization of Health Information Privacy Protections*, 8 CONN. INS. L.J. 283, 293 (2002).

[78] JOINT COMM. ON GOV'T OPERATIONS, LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974: SOURCE BOOK ON PRIVACY 1–9 (1976).

[79] *Id.* at 161–62 (containing the code of fair information practices, which lists the eight principles which guided the creation of the privacy act).

[80] *See infra* notes 81–89 and accompanying text.

The protection afforded by the Privacy Act is insufficient since it applies only to federal agencies.[81] The Privacy Act does not offer protection to individuals from abuse by private sector entities or from government entities at the state level.[82] This boundary of Privacy Act protection renders it ineffective in protecting health information in a healthcare regime dominated by private industry.[83] Moreover, the Privacy Act has often been criticized because it allows federal agencies to hire private database companies to compile, use, and disclose confidential information in ways that would violate the Privacy Act if carried out by a federal agency.[84] Because it regulates only federal agencies, the Privacy Act shifts federal privacy abuses to the private sector, where there is no privacy regulation. Thus, the protection offered by the Privacy Act is minimal in a uniform national health information infrastructure.

Additionally, the Privacy Act is insufficient because it includes many exceptions to its regulations that have been abused and treated as loopholes. Perhaps the most glaring loophole in the Privacy Act is the "Routine Use" exception.[85] This exception allows federal agencies to disclose personal information if they determine that the disclosure is part of the routine use of information and it is compatible with the original purpose for collecting the information.[86] This grants the agency broad discretion to make its own determination regarding the purpose for collecting information and whether the disclosure is compatible with such a purpose.[87]

Another exception allows a federal agency to transfer information to another federal agency upon the written request of the receiving agency.[88] Further, federal agencies are aided in avoiding the Pri-

---

[81] 5 U.S.C. §§ 552(f)(1), 552a(a)(1) (2000).

[82] *See id.*

[83] Pierre, *supra* note 12, at 554–55.

[84] Chris J. Hoofnagle, *Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COMM. REG. 595, 622–23 (2004). The Privacy Act mandates that a private agency hired by contract by a federal agency will be treated as an employee of the federal agency and will be subject to the requirements of the Privacy Act. 5 U.S.C. § 552a(m)(1) (2000). However, the Act specifically exempts a consumer reporting agency from being considered a contractor under this section, and thus, from the requirements of the Privacy Act. *Id.* § 552a(m)(2).

[85] 5 U.S.C. § 552a(b)(3).

[86] *Id.*

[87] *See* DANIEL J. SOLOVE, MARC ROTENBERG & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 583–86 (2d ed. 2006).

[88] 5 U.S.C. § 552a(b)(7).

vacy Act by its vague language and lack of legislative history.[89] Consequently, the Privacy Act cannot be relied upon to protect private medical information.

E. The Health Insurance Portability and Accountability Act

In 1996, Congress passed HIPAA[90] to prevent insurance companies and healthcare providers from abusing the privacy of patients.[91] In its final form, HIPPA includes privacy and security regulations, which attempt to control the use and transmission of heath information.[92] These regulations were meant to establish national minimum standards for health information privacy.[93] Thus, HIPAA establishes a floor for health information privacy but does not preempt stronger state protection.[94] Nevertheless, more adequate standards must be implemented because there are several deficiencies in the HIPAA privacy and security rules.[95]

HIPAA required Congress to pass privacy legislation by 1999 as part of its Administrative Simplification provisions.[96] However, Congress did not carry out this obligation, and the Department of Health and Human Services (HHS) created its own privacy regulations pursuant to HIPAA[97] in 2000, known as the Privacy Rule.[98] Thereafter, HHS received a deluge of comments from the public regarding the complexity of the Privacy Rule, problems with its consent requirement, and the cost of implementing the regulations.[99] Consequently,

---

[89] Haeji Hong, *Dismantling the Private Enforcement of the Privacy Act of 1974:* Doe v. Chao, 38 AKRON L. REV. 71, 86 (2005).

[90] Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 42 U.S.C.).

[91] H.R. REP. NO. 104-496, at 69–70 (1996), *reprinted in* 1996 U.S.C.C.A.N. 1865, 1868–69.

[92] *See* 45 C.F.R. §§ 160.101–164.534 (2007).

[93] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82471 (Dec. 28, 2000).

[94] *Id.*

[95] *See infra* Part II.E.

[96] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, Title II, Subtitle F, §§ 261–264, 110 Stat. 2033. The Administrative Simplification provisions are a portion of HIPAA that were implemented to establish "a national health care fraud and abuse control program." H.R. REP. NO. 104-496, at 67 (1996), *reprinted in* 1996 U.S.C.C.A.N. 1865, 1866.

[97] 42 U.S.C. §§ 1320d to -8 (2000).

[98] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82462.

[99] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53182, 53183, 53209 (Aug. 18, 2002). The consent requirement required cov-

in March 2001, HHS amended the Privacy Rule and allowed the public to comment on proposed regulations.[100] After much debate, the Final Privacy Rule was promulgated in August 2002.[101] The Final Privacy Rule has been criticized for, among other things, its lack of consent requirements that were incorporated in the initial Privacy Rule and for its use of confusing and vague language.[102]

The Final Privacy Rule applies to certain "covered entities," which include health plans, healthcare clearinghouses, and healthcare providers.[103] A "health plan" is a group or individual plan providing or paying for medical care.[104] A "health care clearinghouse" is an entity that processes medical information.[105] Finally, a "health care provider" is an entity that provides "medical or health services" or an entity that "furnishes, bills, or is paid for healthcare in the normal course of business."[106] Moreover, certain "hybrid entities" must comply with HIPAA regulations.[107] A hybrid entity is one that provides healthcare services in addition to several other services.[108] These hybrid entities must comply with the regulations only to the extent that they deal with medical information.[109] Thus, HIPAA protection for medical information applies only to healthcare clearinghouses, healthcare providers, healthcare plans, and to a lesser degree, hybrid entities.

HIPAA privacy regulations apply to all types of "individually identifiable health information," in both electronic and paper form.[110] Individually identifiable information includes information that is created or received by a covered entity and is related to the physical or mental condition of an individual, the "provision of health care to an individual," or the payment for healthcare.[111] The information must either identify an individual or be reasonably traceable to an individual.[112] Individually identifiable information can be

---

ered entities to get the patient's consent before disclosing protected health information for certain uses. *See id.* at 53209.

[100] *Id.*

[101] *Id.* at 53182.

[102] *See* Hoffman & Podgurski, *supra* note 11.

[103] 45 C.F.R. § 160.102 (2007).

[104] *Id.* § 160.103.

[105] *Id.*

[106] *Id.*

[107] *Id.* § 164.504.

[108] *Id.*

[109] 45 C.F.R. § 160.504.

[110] *Id.* § 160.103.

[111] *Id.*

[112] *Id.*

"de-identified," and thus, is not subject to the HIPAA regulations.[113] The definitions for individually identifiable information can be very confusing, and there is little supplemental information guiding covered entities in distinguishing non-identifiable information from individually identifiable information.[114]

HIPAA attempts to safeguard privacy by regulating the circumstances under which individually identifiable information may be used and transmitted. HIPAA allows covered entities to disclose protected health information, without the individual's authorization, to the individual, or for treatment, payment, and healthcare operations.[115] For other disclosures, authorization by the individual is required.[116] Disclosures requiring authorization include disclosures for marketing purposes,[117] disclosure to an employer,[118] and fundraising.[119] Moreover, any use of psychotherapy notes requires authorization by the individual.[120] In the event of a disclosure, the covered entity must also reasonably limit the information disclosed to the minimum amount necessary.[121]

Additionally, the Final Privacy Rule includes the HIPAA Security Rule.[122] The Security Rule mandates that covered entities implement safeguards to protect individually identifiable information transmitted or maintained electronically.[123] The Security Rule is based on

---

[113] *Id.* § 164.502(d)(2).

[114] HHS defines individually identifiable information as "information, including demographic data, that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual." U.S. DEP'T OF HEALTH & HUM. SERVS, SUMMARY OF THE HIPAA PRIVACY RULE 4 (2003), http://www.hhs.gov/ocr/privacysummary.pdf. However, HHS does not explain how to determine whether there is a reasonable basis to believe information can be used to identify the individual. *See id.*

[115] 45 C.F.R. § 164.502.

[116] *Id.* § 164.508.

[117] However, "marketing" does not include marketing of services by the covered entities that are health-related. *Id.* § 164.501. Therefore, if a covered entity seeks to market health-related services to an individual, "the individual cannot opt out or remove herself from the mailing list." SOLOVE ET AL., *supra* note 87, at 383.

[118] This includes employer disclosure used for employment decisions. SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 87, at 383.

[119] *Id.*

[120] *Id.* (citing 45 C.F.R. § 164.508).

[121] 45 C.F.R. § 164.502. This provision does not apply to disclosures to the individual or for the treatment of the individual. SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 87, at 384.

[122] 45 C.F.R. § 164.302–.318 (2007).

[123] *Id.* § 160.103.

four general requirements with which covered entities must comply: (1) to maintain "confidentiality, integrity, and availability" in their electronic health information, (2) to "protect the data against reasonably anticipated threats to its security or integrity," (3) to prevent "impermissible use or disclosure of the information," and (4) to ensure employee compliance with the Security Rule.[124] The Security Rule also requires covered entities to carry out assessments of their compliance with the rule, and to designate a "security official" to manage employee access to health information.[125] A covered entity must be prepared to deal with a security breach and limit its effects.[126] Finally, the Security Rule establishes both physical and technical safeguards to prevent unauthorized access to protected health information.[127] Many of these physical and technical safeguards, however, are addressable and can be waived under various circumstances.[128]

The Final Privacy Rule has been criticized for lacking comprehensive authorization requirements.[129] The Final Privacy Rule requires an individual's authorization for all uses of individually identifiable information, unless used for "treatment, payment, or health care operations."[130] There are, however, various circumstances under which a healthcare provider can condition an individual's treatment on such authorization.[131] Conditioning authorization on treatment can, consequently, cause an ill patient to consent when she normally would not. Additionally, although consent is required for the use and disclosure of protected health information by third parties for marketing purposes,[132] a covered entity can use protected health information to market its own health-related products without authori-

[124] Hoffman & Podgurski, *supra* note 11, at 339 (citing 45 C.F.R. § 164.306(a) (2005)).

[125] 45 C.F.R. § 164.308(a).

[126] *Id.*

[127] *Id.* § 164.310–.312.

[128] Hoffman & Podgurski, *supra* note 11, at 339–40.

[129] *See* June Mary Zekan Makdisi, *Commercial Use of Protected Health Information Under HIPAA's Privacy Rule: Reasonable Disclosure or Disguised Marketing?*, 82 NEB. L. REV. 741 (2004).

[130] SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 87, at 382 (citing 45 C.F.R. § 164.508(a) (2006)).

[131] *Id.* Medical care can be conditioned on research-related disclosure and on the ability to use the information "to determine whether the individual is eligible for benefits or enrollment under a health plan, and for underwriting or risk rating determinations." *Id.* Also, payment for treatment can be conditioned on disclosure so long as disclosure is needed for the payment. *Id.*

[132] 45 C.F.R. § 164.508(a)(3)(i) (2007).

zation.[133] Thus, "a patient cannot opt out or remove herself from the mailing list."[134]

In 2002, the Final Privacy Rule was amended to replace consent requirements with notice requirements for certain uses and disclosures of protected health information.[135] The notice provisions in the Final Privacy Rule are intended to educate patients about privacy rights and concerns, as well as the potential uses of their information.[136] Privacy notices are ineffective for many reasons. First, privacy notices deprive the patient of the ability to discuss the use of her information with employees of the covered entity.[137] Second, covered entities are not required to discuss in the notices any potential uses or disclosures specific to that individual entity.[138] Finally, there is no requirement that patients understand notices, thus covered entities often provide confusing notices to hinder their patients' ability to comprehend the potential uses and disclosures.[139] The result is that notice requirements do little to protect health information privacy.[140]

Furthermore, HIPAA's Security Rule is inoperative against the various threats posed by those seeking to misappropriate personal data.[141] The regulations in the Security Rule allow covered entities broad discretion in implementing their standards.[142] For example, security regulations, which are not mandatory, can be modified or changed depending on the circumstances.[143] As such, covered entities can choose to implement an "equivalent alternative measure" or not to implement the requirement at all if it is not "reasonable and appropriate."[144] Moreover, the regulations are vague and allow an entity to determine what security measures "reasonably and appropriately" meet the implementation standards.[145] Additionally, covered

[133] SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 87, at 383 (citing 45 C.F.R. § 164.501 (2006)).

[134] *Id.*

[135] 45 C.F.R. § 164.520(a) (2007).

[136] Marie C. Pollio, *The Inadequacy of HIPAA's Privacy Rule: The Plain Language Notice of Privacy Practices and Patient Understanding*, 60 N.Y.U. ANN. SURV. AM. L. 579, 592–93 (2004).

[137] *See* Makdisi, *supra* note 129, at 759.

[138] *Id.* The notice requirement only requires entities to disclose "'sufficiently detailed' descriptions of uses and disclosures that are permissible under the rule." *Id.*

[139] *See* Pollio, *supra* note 136.

[140] *Id.*

[141] Hoffman & Podgurski, *supra* note 11, at 336–37.

[142] *Id.* at 337, 350–53.

[143] *Id.* at 339–40.

[144] *Id.* at 339–40, 350–53.

[145] *Id.*

entities are directed to protect the information against "reasonably anticipated threats," and therefore they are left to determine which threats can be reasonably anticipated.[146] The broad discretion given to covered entities, as well as the ability to interpret vague regulations, allows covered entities to decrease privacy protection.[147]

Finally, enforcement of the Privacy Rule is insufficient under HIPAA. HIPAA allows for both civil and criminal penalties against an individual who knowingly obtains or discloses personally identifiable information.[148] In addition, covered entities are liable for disclosures of protected information in violation of the Privacy Rule.[149] However, the Secretary of HHS can only fine covered entities a maximum of $100 per violation, and not more than $25,000 per year for multiple identical violations.[150] Criminal penalties do not apply at all in cases of willful misappropriation by violators who are neither covered entities or employees of covered entities acting within the scope of their employment.[151] Moreover, the Secretary of HHS rarely imposes civil penalties:[152] although HHS received 19,420 complaints between April 2003 and June 2006, it did not issue a single civil fine.[153] Further, HIPAA does not provide for private causes of action, and HHS hearings do not provide monetary damages as a form of relief for harmed individuals.[154]

HIPAA's Privacy Rule, as well as the other privacy protections presently available, will be unable to handle the increased threats to privacy in a national healthcare information infrastructure.[155] The need for enhanced privacy and security protections is exacerbated by the computerization of health records and the increasing centralization of databases.[156] Therefore, any legislation that creates a national, unified healthcare information infrastructure must also include adequate protection.

---

[146] Pierre, *supra* note 12, at 550.

[147] *See* Hoffman & Podgurski, *supra* note 11, at 350–53.

[148] 42 U.S.C. § 1320d-6 (2000).

[149] 45 C.F.R. § 160.400–.426 (2007).

[150] *Id.* § 160.404.

[151] Peter P. Swire, *Justice Department Opinion Undermines Protection of Medical Privacy*, CENTER FOR AMERICAN PROGRESS, June 7, 2005, http://www.americanprogress.org/issues/2005/06/b743281.html.

[152] Hoffman & Podgurski, *supra* note 11, at 357–58.

[153] *Id.*

[154] *Id.*

[155] *See id.* at 384–86.

[156] *See id.*

III. THE FUTURE OF THE ELECTRONIC HEALTH RECORD INFRASTRUCTURE

Several bills have been proposed in Congress to create a unified, national healthcare infrastructure.[157] The central purposes of enacting such legislation are to increase the quality of healthcare and to reduce costs associated with the storage and transmission of health information.[158] These bills, which create a healthcare system more vulnerable to abuse and misappropriation of personal information, typically ignore the enhanced need for privacy protection; instead, they assume that the current scheme of protection will be sufficient.[159] This Part gives an overview of bills that exemplify the current approaches to creating a unified, national healthcare information infrastructure: the Wired for Health Care Quality Act, the Health Information Technology Promotion Act of 2006, and the Independent Health Record Bank Act of 2006. In addition, the bills discussed in this section are also likely to be passed in the near future.[160]

A. Wired for Health Care Quality Act

The Wired for Health Care Quality Act ("Wired Act") is intended to stimulate the creation of a "nationwide, interoperable health information technology system to improve the quality and reduce the costs of health care in the United States."[161] This bill aims to achieve this goal through, among other things, establishing an Office

[157] *See* Independent Health Record Bank Act of 2006, S. 3454, 109th Cong. (2006); Wired for Health Care Quality Act, S. 1418, 109th Cong. (2005); Health Information Technology Promotion Act of 2006, H.R. 4157, 109th Cong. (2005).

[158] *See* S. 3454 ("to improve the exchange of healthcare information through the use of new technology . . . [,]to use such records to build a nationwide health information technology infrastructure, and to promote participation in health information exchange by consumers through tax incentives"); S. 1418 ("To enhance the adoption of a nationwide interoperable health information technology system and to improve the quality and reduce the costs of health care in the United States."); H.R. 4157 ("To promote a better health information system.").

[159] These bills primarily rely on the HIPAA privacy regulations to prevent misuse of personal health information. *See infra* Part II.A–C.

[160] For example, the Wired for Health Care Quality Act has been passed by the Senate and, according to StateNet legislative forecasts, has a ninety-eight percent chance of being passed by a House of Representatives Committee and a ninety-six percent chance of being passed by the House of Representatives. *See* Statenet, Legislative Forecasts, S. 1418, Jan. 10, 2007, http://www.lexisnexis.com (go to "Federal Legal – U.S."; then click "Legislative Histories and Materials"; then search "S. 1418" under "Congressional Bills Legislative Forecasts"). Moreover, the Health Information Promotion Act of 2005 was passed in the House of Representatives on July 27, 2006. *See* H. Roll No. 416 (2006).

[161] S. 1418, 109th Cong. (2005).

of the National Coordinator for Health Information Technology (ONC) within the Office of the Secretary of HHS[162] to coordinate the adoption of uniform electronic health information standards; establishing an American Health Information Collaborative to promulgate recommendations to be considered by various federal agencies;[163] and by providing grants to private entities for compliance with the bill.[164] The Wired Act was introduced by Senator Enzi of Wyoming on July 18, 2005, and was passed by the Senate on November 17, 2005.[165] Although the bill includes provisions protecting private health information, they are insufficient for the uniform health information infrastructure that the bill attempts to establish.

Initially, the bill defines various terms to provide guidance and elucidate the scope of its provisions.[166] The bill defines the term "Health Care Provider" to include hospitals, skilled nursing facilities, home health entities, healthcare clinics, group practices, pharmacies, laboratories, physicians, and any other entities determined appropriate by the Secretary of HHS.[167] This definition is more specific than that in HIPAA[168] and is broad in scope since the Secretary of HHS has the ability to include additional entities.[169] Additionally, it is notable that the bill defines "Qualified Health Information Technology" as a "computerized system" that "protects the privacy and security of health information," allows permitted access to electronic health information, "incorporates decision support to reduce medical errors," and complies with standards under the bill.[170]

Thereafter, this bill provides that the ONC would be headed by a "National Coordinator" to be appointed by and report to the Secretary of HHS.[171] The duties of the ONC would entail coordinating federal agencies and private entities in developing a national health information infrastructure to protect patients' individually identifiable information, improve the quality of healthcare, reduce medical er-

[162] *Id.* § 2902.

[163] *Id.* § 2903.

[164] *Id.* §§ 2904–2906.

[165] Congressional Information Service, Bill Tracking Report, S. 1418, 2005, http://www.lexisnexis.com (go to "Federal Legal – U.S."; then click "Legislative Histories and Materials"; then search "S. 1418" under "Bill Tracking Report-Current Congress").

[166] S. 1418 § 2901.

[167] *Id.* § 2901(1).

[168] 45 C.F.R. § 160.103 (2007).

[169] S. 1418 § 2901(1).

[170] *Id.* § 2901(6).

[171] *Id.* § 2902(a).

rors, reduce healthcare costs, facilitate the exchange of information between entities, and facilitate medical research.[172] Moreover, the National Coordinator of the ONC would directly advise the Secretary of HHS and the President.[173] The ONC will also be allowed to request federal agencies to assign their employees to the office for assistance in achieving its goals.[174]

Next, the bill would establish the American Health Information Collaborative (AHIC), a quasi-public organization that will serve as a forum for discussing issues related to establishing and implementing an interoperable healthcare infrastructure and for "recommend[ing] . . . standards for the electronic exchange of health[care] information."[175] The AHIC would be composed of an even distribution of representatives from "consumer or patient organizations," healthcare providers, health insurance plans, third-party payors, information technology vendors, privacy and security organizations, and purchasers or employers.[176] Moreover, the representatives would serve for a maximum of two years.[177] The AHIC would be responsible for submitting annual policy recommendations to increase system efficiency and security.[178] Thereafter, HHS and other federal agencies would review these recommendations and determine whether they should be implemented by the federal government.[179] These regulations would only govern federal agencies and would be entirely voluntary for private entities.[180]

The Wired Act includes many provisions aimed at protecting individually identifiable health information from wrongful use and disclosure.[181] However, there are several reasons why this bill lacks adequate privacy protection. The main deficiency is that the regulations would be mandatory only for federal agencies.[182] Regulation of the private sector is premised on the belief that private entities will *voluntarily* abide by the standards set forth by HHS and the AHIC.[183] However, it is naïve to expect private entities to voluntarily incur the sub-

[172] *Id.* § 2902(b)(1)–(9).
[173] *Id.* § 2902(c).
[174] *Id.* § 2902(d).
[175] S. 1418 § 2903(a)(3).
[176] *Id.* § 2903(b).
[177] *Id.*
[178] *Id.* § 2903(c)–(d).
[179] *Id.* § 2903(e).
[180] *Id.* § 2903(h).
[181] *See* S. 1418 § 2903(h).
[182] *Id.*
[183] *Id.*

stantial costs of purchasing new technology and implementing administrative standards.[184] Moreover, as has been shown in previous Parts of this Comment, allowing private industry to regulate itself typically results in lenient standards and a lack of adequate protection.[185] Thus, this bill is as limited in protecting information in the private sector as is the Privacy Act of 1974. Moreover, the Wired Act's attempt to create a seamless, uniform infrastructure for the storage and transmission of electronic health information will be hindered because it fails to apply the regulations to private industry. The result would be a uniform, national *federal agency* infrastructure, with vast differences between public and private standards. Consequently, the bill's ability to protect private information would be frustrated, since electronic health information that is highly guarded by a federal agency may be misappropriated when it is transferred to a private entity. It is unlikely that this system would allay public fears of inappropriate use of health information that cause patients to withhold information from practitioners.[186] Therefore, to be effective, the Wired Act must make its regulations mandatory for private entities.

B. Health Information Technology Promotion Act of 2006

The Health Information Technology Promotion Act of 2006 (HITPA) was introduced on October 27, 2005, by Representative Johnson of Connecticut to "promote a better health information system."[187] The bill was subsequently passed by the House of Representatives.[188] HITPA requires standards to be promulgated by the federal government regarding the adoption and implementation of improved technology to create a uniform, national health information infrastructure.[189] However, the bill would establish few privacy safeguards and is insufficient to protect individuals' private information from misappropriation.

---

[184] The Wired Act allows for federal grants to healthcare providers for implementing the regulations and purchasing new technology resulting from the AHIC's recommendations. *Id.* § 2905. However, to receive these grants, healthcare providers must meet various requirements and must also spend one dollar on implementation and new technology for every three dollars in government grants. *Id.* Therefore, even in the event that a healthcare provider obtains a government grant, it must still voluntarily choose to pay large sums of money to implement these standards.

[185] *See supra* Part II.E.

[186] *See supra* notes 35–41 and accompanying text.

[187] *See* Health Information Technology Promotion Act of 2006, H.R. 4157, 109th Cong. (2005).

[188] H. Roll No. 416 (2006).

[189] *See* H.R. 4157 § 103.

HITPA delineates a paradigm for the creation of a unified, national interoperable health information infrastructure similar to that detailed in the Wired Act.[190] HITPA would establish the Office of the National Coordinator for Health Information Technology for essentially the same purposes as described above.[191] Additionally, this bill would require the National Coordinator to advise the Office of Management and Budget on health information issues and to be the "promoter of health information technology in medically underserved communities."[192] Further, the bill would require the American Health Information Community to submit a report on the state of the health information infrastructure and to make recommendations.[193] The bill recommends that measures should be taken to establish the American Health Information Community as a more "permanent advisory and facilitation entity."[194]

The bill further delineates the process by which the National Coordinator, working with the American Health Information Community, would promulgate guidelines to promote a national healthcare infrastructure.[195] The National Coordinator must first produce a "strategic plan" with a schedule for analyzing and endorsing "core interoperability guidelines" for "significant use cases."[196] A "core interoperability guideline" is defined as "a guideline to improve and promote the interoperability of health information technology" that "the National Coordinator determines is essential and necessary."[197] Moreover, a "significant use case" is "a category (as specified by the National Coordinator) that identifies a significant use or purpose for the interoperability of health information technology" including purposes such as transmitting laboratory information and health records.[198] The National Coordinator would then, consistent with the schedule, endorse certain core interoperability guidelines.[199] Subsequently, these guidelines would be sent to the President, who must ensure compliance by federal agencies that broadly collect or submit

[190] *Compare* H.R. 4157, *with* Wired for Health Care Quality Act, S. 1418, 109th Cong. (2005).
[191] H.R. 4157 § 101.
[192] *Id.*
[193] *Id.* § 102.
[194] *Id.*
[195] *Id.* § 103.
[196] *Id.*
[197] H.R. 4157 § 103.
[198] *Id.*
[199] *Id.*

health information.[200] Beyond this, however, adherence to the guidelines would be entirely voluntary for federal agencies and private entities.[201]

HITPA also includes provisions for updating standards for electronic exchanges, providing incentives for physicians to implement new technology, and conducting studies on various aspects of health information technology.[202] The bill would establish a method by which standard-setting organizations may attain expedited implementation of upgrades or additions to data transmission standards.[203] Standard-setting organizations would be able to notify the Secretary of HHS that they are upgrading or improving their codes or formats for transmitting health information, and the Secretary would then publish a notice in the Federal Register,[204] and allow the public to comment on the proposal.[205] Next, the Committee on Vital Health Statistics would hold a hearing, which would include testimony from the public.[206] The Committee would then deliver recommendations to the Secretary regarding adoption of the upgrade or improvement.[207] Finally, the Secretary would determine whether these changes should be implemented.[208] This allows for expedited implementation of the newest and most advanced standards for the transmission of health-related data.[209] Additionally, HITPA would provide safe-harbor provisions to anti-kickback civil and criminal penalties and exemptions from physician referral limitations "for [the] provision of health information technology and training services" to encourage physicians to adopt new technology.[210] Moreover, the bill would require studies on the impact of health information technology in certain areas of healthcare and the likelihood that certain changes to the healthcare system will be successful.[211] Among other things, these studies would examine the need for unification of

[200] *Id.* Federal agencies broadly collecting and submitting health information must be in compliance with these guidelines within three years of their endorsement by the National Coordinator. *Id.*

[201] *Id.*

[202] *See id.* §§ 201–407 (2005).

[203] H.R. 4157 § 201.

[204] *Id.*

[205] *Id.*

[206] *Id.*

[207] *Id.*

[208] *Id.*

[209] H.R. 4157 § 201.

[210] *Id.* §§ 301–302.

[211] *Id.* §§ 401–407.

state laws,[212] the ability to integrate health information technology in home healthcare,[213] and the methods through which to use health information technology to manage chronic diseases.[214] This combination of provisions seems to be aimed toward encouraging physicians and healthcare providers to adopt technology that is current and adequately suited to the needs of the healthcare industry.

HITPA cannot be expected to realistically induce the creation of a unified, interoperable healthcare system with proper security and privacy protections. Although the bill does mention maintaining privacy and security in health information, it does little to ensure that, if enacted, privacy and security regulations will be promulgated.[215] The bill focuses almost entirely on improving efficiency in the healthcare industry without significantly considering health information privacy and security concerns.[216] The bill never mentions any specific privacy or security measures to counteract the increased threats incident to a unified, national health information infrastructure.

Moreover, the scope of any privacy regulations would be extremely limited. The regulations promulgated by the Secretary of HHS would only be applied to selected federal agencies through the actions of the President.[217] Further, these agencies would have three years to comply with such regulations.[218] It is absurd to believe that this three-year lag-time will not circumvent the bill's attempt to ensure the use of the most current technology through expedited endorsement of improvements to data transmission standards.[219] As mentioned above in the analysis of the Wired Act,[220] it is also nonsensical to expect private industry to expend considerable resources on voluntary privacy and security regulations. Therefore, any privacy or security regulations promulgated pursuant to this bill would not be applied to adequately protect the privacy of sensitive health information. Consequently, this bill would not increase efficiency in the healthcare system by reducing the amount of information withheld

---

[212] *Id.* § 401.

[213] *Id.* § 402.

[214] *Id.* § 407.

[215] *See* H.R. 4157 §§ 101–102.

[216] *Id.* § 101. The Act lists providing for the "confidentiality and security of individually identifiable health information" eighth on a list of thirteen goals of a "Nationwide Interoperable Health Information Technology Infrastructure." *Id.*

[217] *Id.* § 103.

[218] *Id.*

[219] *Id.* § 201.

[220] *See supra* Part III.A.

by members of the public from medical practitioners due to fears of misappropriation.

C. *Independent Health Record Bank Act of 2006*

Introduced on June 6, 2006, by Senator Sam Brownback of Kansas, the Independent Health Record Bank Act of 2006 (IHRBA) would establish and utilize a unique system of independent health record banks to create a national healthcare infrastructure.[221] This bill would also encourage participation by individuals, healthcare providers, and employers through a series of tax incentives[222] and through health record banks sharing their revenue.[223] A few purposes of this health information infrastructure are to improve healthcare quality, to promote disease prevention and management of chronic illnesses, to ensure that medical information is available for decision making, to increase the efficiency and reduce the cost of healthcare, and to ensure confidentiality of individually identifiable information.[224]

Within a year of Congressional enactment of this bill, the Secretary of Commerce must promulgate standards for "the establishment and certification of independent health record banks."[225] Record banks would hold lifetime electronic health records for their members, and would be interconnected to form a "national health information network."[226] Moreover, these health records "may contain health plan and debit card functionality."[227] Record banks would be treated as covered entities under HIPAA, and may carry out healthcare clearinghouse activities.[228] Additionally, IHRBA would require record banks to be non-profit entities,[229] and not deny membership to any individual.[230]

Record banks would be able to finance their activities in various ways. First, record banks could charge healthcare entities and individual account holders fees for using the bank.[231] Second, they could sell non-identifiable and partially identifiable health information to

---

[221] Independent Health Record Bank Act of 2006, S. 3454, 109th Cong. (2006).
[222] *Id.* § 4(a)(4)–(5), (e)(3).
[223] *Id.* § 4(e)(2).
[224] *Id.* § 2.
[225] *Id.* § 4.
[226] *Id.*
[227] S. 3454 § 4(a).
[228] *Id.* §§ 4(b), 5.
[229] *Id.* § 4(b).
[230] *Id.* § 4(c).
[231] *Id.* § 4(e).

research facilities.[232] Finally, they could generate revenue through "any other activities determined appropriate by the Secretary [of Commerce]."[233] However, a record bank would have to share any revenue that it accumulates with account holders, and may share its revenue with healthcare providers and payers.[234]

IHRBA would limit the disclosures of health information that record banks may make.[235] Generally, a record bank could only disclose an individual's independent health record with the prior consent of the individual.[236] Moreover, a record bank would have to comply with the provisions of the HIPAA Privacy Rule.[237] However, there is an exception to the consent requirement for emergency situations.[238] A record bank could allow healthcare providers to access "a limited, authenticated data set concerning an individual for emergency response purposes" during an emergency room visit, without prior consent from the individual.[239] In addition, when selling health information, a record bank may only disclose an individual's non-identifiable or partially identifiable health information upon meeting several requirements.[240] The record bank and the individual must agree to any such sale.[241]

IHRBA would afford individual consumers certain rights regarding their independent health record.[242] The individual would maintain ownership over his or her complete health record, and would have the right to review it at any time.[243] Further, the individual would be able to add information to his or her health record, and could seek to amend information in his or her record according to standards to be prescribed by the Secretary of Commerce.[244] However, the healthcare entity "shall serve as the custodian of . . . information that has been added by such entity to the health record of an individual."[245]

---

[232] *Id.*

[233] S. 3454 § 4(e).

[234] *Id.*

[235] *See id.* §§ 4(d), 6.

[236] *Id.* § 6(a).

[237] *Id.* § 6(d).

[238] *Id.* § 6(c)(2).

[239] S. 3454 § 6(c)(2).

[240] *Id.* § 6(b)(1)–(7).

[241] *Id.* § 6(b)(1).

[242] *Id.* § 4(d)(1).

[243] *Id.* The individual can review the contents of his or her health record "at any time during the normal business operating hours of the bank." *Id.*

[244] *Id.*

[245] S. 3454 § 4(d)(2).

IHRBA includes several incentives to encourage participation in the health record bank system by individuals, employers, and healthcare entities. As mentioned above, the bill would require record banks to share any revenue resulting from the sale of health information with its members.[246] A record bank could also share this revenue with healthcare providers.[247] The bill would make this even more lucrative by exempting the revenue from taxable income under the Internal Revenue Code.[248] Thus, individuals and healthcare providers would contribute more information to electronic health records to make them as valuable as possible.[249] Additionally, IHRBA would amend the Internal Revenue Code to allow employers a tax credit for up to fifty dollars per employee for any investments made to maintain that employee's independent health record.[250] This would encourage employer and employee participation in independent health record banks.[251]

Finally, IHRBA includes measures to assure compliance with the bill and its regulations. First, IHRBA includes provisions for regulatory oversight of record banks.[252] The bill would require the Secretary of Commerce to "develop a program to certify entities to operate independent health record banks," to track economic activity of record banks, and to establish an "interagency council" to audit record banks.[253] The interagency counsel would be responsible for auditing record banks and recommending privacy and security protections.[254] These protections would include record banks notifying individuals when their privacy is breached, implementing security measures to restrict access to information, and analyzing the risk of a security breach.[255] Second, IHRBA would require states to establish a state agency to address complaints by state residents pertaining to a record bank.[256] Moreover, record banks would have to provide these state agencies with information regarding the record bank's policies and regarding its use and storage of information.[257] Third, IHRBA would

[246] *Id.* § 4(e).
[247] *Id.*
[248] *Id.*
[249] *Id.* § 4(a)(5).
[250] *Id.* § 10.
[251] S. 3454 § 4(a)(4).
[252] *Id.* § 8.
[253] *Id.* § 8(a).
[254] *Id.* § 8(b).
[255] *Id.*
[256] *Id.* § 7(b).
[257] S. 3454 § 7(b).

attempt to ensure compliance by making civil and criminal penalties available for wrongful disclosure by a record bank.[258] IHRBA would do this by applying HIPAA civil and criminal penalties[259] to record banks.[260] Finally, IHRBA would subject record banks' transmission and use of data to all applicable existing federal and state privacy and security protections.[261]

IHRBA commodifies personal health information on a scale never before attempted in the United States. This bill seeks to establish record banks throughout the United States,[262] and would give individuals a property right in their health information.[263] Such a system could greatly increase efficiency in the healthcare system while protecting privacy. This type of system, however, raises various concerns regarding its effectiveness and privacy. For one thing, commentators have criticized granting a privacy right in personal information.[264] Moreover, the increasing value of electronic health records augments the incentives for misappropriation. Finally, reliance on the HIPAA Privacy Rule would be grossly inadequate under this regime. HIPAA allows a healthcare provider to condition treatment of an individual on that individual's authorizing the healthcare provider to disclose the individual's medical information to research facilities.[265] Thus, a healthcare provider would be able to sell the information directly to a research facility and effectively cut out the record bank middle-man.[266] This would result in a loss of revenue to record banks and individuals,[267] which would negate the incentives for individual and healthcare provider participation in record banks.[268] IHRBA would be successful only if it includes additional pri-

[258] *Id.* § 9.

[259] 42. U.S.C. § 1320d-6 (2003).

[260] S. 3454 § 9.

[261] *Id.* § 7(a).

[262] *Id.* § 2. The purpose of the Act is to create a "nationwide health information technology network, which implies that the record banks will be established throughout the nation." *Id.*

[263] *Id.* § 4(d)(1)(a).

[264] *See infra* Part IV (discussing the use of a property right in one's personal health information).

[265] *See* 45 C.F.R. § 164.508(b)(4).

[266] *Compare id.* (explaining that HIPAA can condition treatment on patient authorization for research related disclosure), *with* S. 3454 §§ 4(e)(b), 6(b) (allowing banks to generate revenue through the sale of non-identifiable and partially identifiable information to third parties for research).

[267] *See* S. 3454 §§ 4(e)(b), 6(b).

[268] *Id.* § 4(e).

vacy regulations and security protections to ensure that all personal health information flows through the record banks securely.

IV. SOLUTION

A uniform, national health information infrastructure must employ a combination of methods to protect the privacy of personal health information. A variety of methods are available for Congress to implement in its legislation.[269] Substantially all of these methods, however, have been criticized as being flawed in one way or another. Thus, with the ever-increasing need for privacy protection, a solution exists in employing a variety of these safeguards to provide layers of protection, with each layer guarding against the inadequacy of other layers.

The basis for a novel privacy protection paradigm can be the recognition of a property right in one's own health information. Although the commoditization of health information as a property right has often been criticized, there are solutions to the problems inherent in such commoditization. Consequently, applying these solutions allows the benefits of such a system to outweigh the negative consequences.

First, it has been said that free alienability hinders the effectiveness of using a property right to protect information privacy.[270] The right of a property owner to freely transfer property rights to third parties is a fundamental aspect of property law.[271] Thus, 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.[272] Second, it has been claimed that the commoditization of information will result in information market failure, which will cause people to trade away too much personal information.[273] Thus, it is claimed that utilizing property rights in personal information will increase trading in personal information, and as a result, privacy will be reduced.[274] Finally, critics

[269] These methods include property rights, contractual protection, common law or statutory causes of action, and criminal penalties. *See infra* Part IV.

[270] Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1137–47 (2000).

[271] *Id.*

[272] *Id.*

[273] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2076–84 (2004).

[274] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423–28 (2000).

argue that recognizing property rights in personal information is contrary to a public benefit that exists from privacy protection.[275] Creating a property right in personal information has been described as "anathema" and as "morally obnoxious."[276] Moreover, it has been said that propertizing personal information "may make no more sense . . . than . . . to commodify voting rights."[277] Although there has been much criticism of propertizing personal information, there are significant benefits to utilizing property rights to protect such information.[278]

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. A common feature of current privacy protection is that it relies on liability rules.[279] Under a liability rule, privacy is invaded, followed by some type of legal recourse, and thereafter, the privacy invader pays a price for obtaining the information.[280] Under a property scheme, however, the owner of a property right is able to negotiate the sale of that person's information.[281] Moreover, the pre-sale negotiation pursuant to a property regime allows the individual to determine the value of the individual's information. Therefore, the value of one's privacy will not be determined by a data collector, court, or legislative body as in a liability regime.[282] Although such a system could lead to personal information becoming under-valued and sold at too low of a price, it would be possible for 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.

Additional benefits of a property regime include forcing businesses to internalize externalities associated with data collection as well as property rights running with the property. Requiring businesses to internalize the costs associated with information gathering leads to more prudent decision-making regarding the collection and use of personal information.[283] Therefore, the propertization of data may lead to a reduction in the overall amount of data being col-

[275] Schwartz, *supra* note 273, at 2084–90.

[276] Samuelson, *supra* note 270, at 1143.

[277] *Id.*

[278] *See infra* notes 279–85 and accompanying text (discussing the benefits of using property rights to protect personal information).

[279] LAWRENCE LESSIG, CODE VERSION 2.2, at 279–80 (2006).

[280] *See id.*

[281] *See id.*

[282] *See id.*

[283] McClurg, *supra* note 28, at 91–92.

lected.[284] Propertization will also result in individuals receiving a pecuniary benefit in exchange for the use of their personal information. Additionally, limitations on property rights will run with the property interest, and therefore, protection will apply to third parties.[285]

The problems caused by free alienability inherent in a property-based privacy protection regime may be answered with a somewhat obvious solution: restricting alienability. Although privacy critics argue that free alienability is a fundamental principle in privacy law and therefore unavoidably hinders utilization of property rights to protect privacy,[286] restrictions on alienability are equally fundamental aspects of intellectual property.[287] Paul Schwartz, a leading privacy advocate, compares limited alienability of an information property right to the successful restrictions on alienability allowed in modern copyright law.[288] Correspondingly, Schwartz proposes a "model of propertized personal information" which relies on "hybrid inalienability."[289] This model "unpack[s]" the "bundle of sticks" commonly associated with a property right and puts limits on the rights of use and transferability in the property that "follow[] personal information through downstream transfers and limit[] the negative effects that result from 'one-shot' permission to all personal data trade."[290] Therefore, legislation creating a uniform national healthcare infrastructure will be able to adequately restrict alienability, assuming healthcare entities comply with the applicable statutes and regulations.

The advent of a health information property regime facilitates, and increases the efficacy of, the second "layer" of health information privacy protection: safeguarding privacy through contract.[291] Traditionally, the formation of a contract includes two or more parties bargaining to exchange consideration, making offers and counteroffers, and subsequently agreeing to and accepting the terms of the contract.[292] Ideally, then, the use of contracts to protect privacy

---

[284] *Id.*

[285] *See* notes 291–303 and accompanying text (discussing limitations of contract-based privacy protections).

[286] Schwartz, *supra* note 273, at 2091. Free alienability "is considered by many to be an inevitable aspect of property." *Id.*

[287] *Id.* at 2092; *see also* Jacqueline Lipton, *A Framework for Information Law and Policy*, 82 OR. L. REV. 695, 729 (2003).

[288] Schwartz, *supra* note 273, at 2092.

[289] *Id.* at 2094.

[290] *Id.* at 2094–96.

[291] *See infra* notes 292–93 and accompanying text (discussing the use of property as consideration).

[292] CHARLES L. KNAPP, NATHAN M. CRYSTAL & HARRY G. PRINCE, PROBLEMS IN CONTRACT LAW: CASES AND MATERIALS, 1–161 (5th ed. 2003).

should allow the individual and the entity seeking to use the information to bargain and come to an agreement on the terms of the contract. Thus, using a property right as consideration, an individual should be able to tailor an entity's use of the property to suit his or her needs, and will not agree to unsuitable terms. However, data collecting entities typically use adhesion contracts, leaving little or no opportunity for bargaining.[293] Many healthcare entities already use confusing language in their privacy notices, causing patients to be unaware of their rights and the entity's potential uses of their personal information.[294] Consequently, information-gathering entities effectively coerce individuals to consent to unfair terms.[295] Moreover, many information gatherers include provisions enabling the entities to change the terms in their privacy policies at random.[296] Therefore, many argue that legislatures must adopt default rules in information privacy contracts, typically utilizing opt-in requirements in order to deviate from the default.[297] Using default rules will shield unsuspecting individuals from releasing their rights unwillingly. Consequently, they will restore an individual's ability to bargain for favorable contract terms.[298]

Additionally, when an individual uses the law of contracts to protect privacy, the extent of the protection afforded by the contract is limited to enforcement against those parties who are in privity of contract with the individual.[299] Thus, a third party cannot be sued under contract law for appropriating data given as consideration pursuant to a contract.[300] For example, a data collecting entity could freely transfer the rights granted to it pursuant to a contract to a third party, and the original party to the contract would have no rights against that third party. However, if a property right is recognized in personal information, then third parties would not be immune from suit from the original "owners" due to the fundamental principle that

[293] Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1265 (1998).

[294] *See* Pollio, *supra* note 136, at 593.

[295] *See* Kang, *supra* note 293, at 1265.

[296] Schwartz, *supra* note 273, at 2080.

[297] *See* Kang, *supra* note 293, at 1270–72; Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2416–17 (1996); Schwartz, *supra* note 273, at 2100–06.

[298] *See* Murphy, *supra* note 297, at 2404–16 (analyzing empirical data showing the efficiency and lowered transaction costs associated with using contractual default rules to protect information privacy).

[299] KNAPP, CRYSTAL & PRINCE, *supra* note 292, at 494.

[300] *See id.*

property rights run with the property interest.[301] This means that property rights "can be enforced against subsequent transferees of other rights in the [personal information]."[302] Moreover, third parties will not be allowed an interest in property granted by a second party without the authority to make such a grant.[303] By creating a property right, the first "layer" of protection under this Comment's proposed paradigm partially safeguards against the inadequacies of contractual privacy protection.

Nevertheless, it is naïve to conclude that a property right in personal information is sufficient to contain such information within the realm of contractually bound second parties.[304] Consequently, tort liability for misappropriation must serve as a third "layer" of protection. Without a private cause of action for misappropriation, there is little to stop entities from wrongfully obtaining information from individuals, as well as from second parties. For example, as mentioned in the foregoing paragraph, a secondary party cannot grant to a third party a greater property interest than that which it owns. Thus, if a second party disregards a restriction on alienability and subsequently transfers its property interest to a third party, the third party's interest is voided. This works well for property interests in land or other tangible property, but it disintegrates when dealing with intangible property, such as personal information.[305] Consequently, attaching civil liability to third-party misappropriation is necessary to deter prohibited use and acquisition.

Somewhat counter-intuitively, tort litigation may increase the efficiency of this privacy protection scheme. First, although transaction costs associated with complex litigation may commonly reduce efficiency, those transaction costs, in addition to any ensuing civil damages, have the effect of deterring misappropriation.[306] Second, allow-

[301] Henry Hansmann & Reinier Kraakman, *Property, Contract, and Verification: The Numerous Clauses Problem and the Divisibility of Rights*, 31 J. LEGAL STUD. 373, 374 (2002).

[302] *Id.*

[303] *See id.* at 375.

[304] *See* McClurg, *supra* note 28, at 96–97.

[305] The reason is that the holder of intangible, intellectual property may freely alienate such property while retaining the entire, original interest. *See* Lipton, *supra* note 287, at 728–36. It is very difficult to retake possession of private information once it has been disclosed because it is intangible. *See id.* Indeed, a third party wrongfully obtaining personal information might not abide by contractual restrictions on use that bound the second party, since the third party is not in privity with the original owner. *See supra* notes 291–303 and accompanying text (discussing the limitations of contractual privacy protection).

[306] McClurg, *supra* note 28, at 101.

ing injured parties to seek compensation assures that motivated plaintiffs will aggressively pursue claims against the entities that caused their harm.[307] Plaintiffs seeking "personal justice and redress" are in a better position for success than, for example, members of a government regulatory agency.[308] Third, civil discovery pursuant to a lawsuit is more likely to yield information pertaining to the violative practices of an entity than an investigation by a federal agency.[309] This is evidenced by the current dearth of knowledge about the secretive practices of information gathering entities.[310] Finally, assuming the privacy claims would meet the requirements for class action certification, having a private cause of action would allow plaintiffs to aggregate their claims. Consequently, individual harms that are too minor to be worth the costs of litigation may be aggregated to make litigation profitable.[311] Thus, under a tort liability scheme, entities are deterred from harming vast numbers of individuals in such a minor way as to avoid liability. Further, unlike other methods of privacy protection, creating a private cause of action is relatively easy and in-

---

[307] *Id.* at 100.

[308] *Id.*

> [L]egislation would probably not be effective in controlling information privacy unless it created a strong incentive for someone to enforce it. . . . If congressional committees and regulatory agencies are the sheriff, tort plaintiffs and their lawyers are the bounty hunters. People who have a personal stake in the outcome have a much stronger incentive to influence the outcome . . . .

Id. (citations omitted).

[309] *Id.* at 99.

> Conventional wisdom says that legislative and agency bodies are better venues for collecting information about social policy issues. At least in the context of consumer data, that view may be wrong. Studying transcripts of the FTC's major "workshop" on consumer data fails to answer the most important questions regarding data mining and profiling. Most notably, not a single sample of a consumer data profile was produced at the workshop, despite vigorous attempts by a leading privacy advocate to obtain profile samples in advance. The workshop transcript reflects amiability among the participants that is ill-suited to the goal of meaningful fact finding. For the most part, these agency investigators pitched softball questions that industry representatives safely bunted with vague answers.
>
> Civil discovery in the U.S. is an extremely liberal process that allows broad inquiries in an attempt to ferret out relevant facts. The civil discovery process, backed up by the power of court orders, including the potential for sanctions, can be a much more potent method of fact investigation than government hearings.

Id. (citations omitted).

[310] McClurg, *supra* note 28, at 98–99.

[311] WILLIAM T. ALLEN & REINIER KRAAKMAN, COMMENTARIES AND CASES ON THE LAW OF BUSINESS ORGANIZATION 351–52 (2003).

expensive.[312] Legislation may create a private cause of action by merely including a provision stating that one shall exist. Moreover, courts are free to create a common law cause of action to deal with misappropriation.[313] Hence, a private cause of action should be created to supplement any legislation creating a unified national health information infrastructure.

V. CONCLUSION

The right to health information privacy, deemed "sacred" by the Supreme Court,[314] is being whittled away by legislation containing little or no privacy protection.[315] It has been shown that misappropriation and wrongful disclosure of private health information can have devastating consequences.[316] Nevertheless, Congress has focused almost exclusively on increasing efficiency in healthcare, ignoring the potential harm caused by inadequate privacy protection.

This Comment, while recognizing that no conventional method of privacy protection is flawless, proposes a regime that relies on three layers of protection, so that the inadequacies of each is counteracted by the strengths of the others. Consequently, this paradigm ensures adequate protection in a national, unified health information infrastructure.

---

[312] McClurg, *supra* note 28, at 97–98.

[313] *Id.*

[314] Union Pac. Ry. v. Botsford, 141 U.S. 250, 251 (1891).

[315] *See supra* Part III.A–C.

[316] *See supra* Part II.A.