Electronic Health Records and Respect for Patient Privacy: A Prescription for Compatibility

ABSTRACT

Thousands of years ago in ancient Greece, Hippocrates, the “father of Western Medicine,” created the first health record. Although the medical field advanced remarkably from Hippocrates’ time to the mid-twentieth century, medical records still shared at least two common features: They were written by the hand of a physician and kept in a tangible medium. The early 1960s witnessed the advent of a new kind of health record—the electronic health record (EHR)—a longitudinal, electronic record of a patient’s entire health history. Since the latter half of the twentieth century, scientists, computer technicians, universities, healthcare providers, and the government have been working toward the digitization of health records. Finally in 2009, Barack Obama pledged that by 2014, all American health records would exist in an electronic format. As part of this undertaking, the federal government has earmarked $19.2 billion in incentives for medical institutions to invest in EHRs via the American Reinvestment and Recovery Act (ARRA).

At first blush, given our increasing dependence on and affinity for electronics, it may seem that EHRs are a great advancement for the medical field. However, there may be an Achilles heel of EHRs: patient privacy. Opponents of EHRs argue that by making health records completely digital, we are entrusting our most private and potentially compromising information to “black boxes” and opening ourselves up to privacy breaches. Out of this grave concern comes the most pertinent question in the debate over digitalization: Are EHRs and patient privacy mutually exclusive?

This Note argues that despite the concerns of EHR critics, patient privacy and a digital record system may peacefully coexist. To ensure that privacy is maintained, physicians, information technology specialists, hospital personnel, the federal government, and patients must work together to implement the necessary safeguards for a successful and secure EHR system. While it may never be possible to ensure the absolute security of all health information stored in
cyberspace, this Note will argue that a collaborative effort can at least guarantee that personal health information is protected long beyond 2014.

TABLE OF CONTENTS

I. EXPLORING A NEW MEDICAL CHART: ELECTRONIC HEALTH RECORDS ................................................................. 444
   A. What is an Electronic Health Record? ........................................ 444
   B. Medical Records ................................................................. 445
   C. Privacy Regulations and the Health Insurance Portability and Accountability Act ......................................................... 447
      1. Introduction to Privacy Regulations .................................... 447
      2. An Overview of HIPAA ...................................................... 448
      3. The HIPAA Privacy Rule .................................................... 450
      4. HIPAA and EHRs ............................................................ 452

II. A HEALTHY DEBATE: EXALTING ACCESS OR PRAISING PRIVACY? ........................................................................... 455
    A. The Problem of Privacy: The Case Against EHRs ..................... 455
    B. Protecting Privacy: The Case Against the Case Against EHRs .......... 458

III. A PRESCRIPTION FOR PRIVACY .......................................................................................................................... 460

IV. CONCLUSION ............................................................................................................................................................... 462

In a speech to students at George Mason University on January 8, 2009, Barack Obama advocated for immediate action on the American Recovery and Reinvestment Plan that would save or create over three million jobs, while at the same time investing in health care, energy, and education in order to spark the floundering American economy.\(^1\) In this same speech, the President pledged that within five years—by 2014—all of America’s health records would exist in an electronic format.\(^2\) As part of this undertaking, the Obama Administration has since earmarked $19.2 billion in incentives for medical institutions, doctors, and other healthcare providers to invest in electronic health records, with two conditions: Recipients must meet certain standards and show ‘meaningful use’ of the funds.\(^3\)

---

2. Id.
The debate over digitizing health records is not new to the political arena. The change in administration and rising unrest with the American system of health care, however, has pushed the debate over electronic health records to the forefront of the country’s political agenda. With the political will of this administration behind it, the government should seize the opportunity to craft a safe and secure electronic health record system that garners the confidence of the American people.4

The debate over electronic health records (also known as EHRs) brings with it not only economic and political implications, but personal and social ones as well. Proponents of EHRs tout their numerous potential benefits: significant economic savings to the health care industry, United States Government, and patients; easier transfer of records between medical offices; a reduction in duplicative tests and procedures; better and more thorough medical care for patients; and an overall improvement in safety, quality, and efficiency of medical care.5 President Obama himself noted that the shift to electronic health records would not “just save billions of dollars and thousands of jobs. It will save lives by reducing the deadly but preventable medical errors that pervade the American healthcare system.”6 However, making patients’ health records accessible at the click of a mouse invites questions and criticisms. Most notably, opponents of EHRs cite breaches of patient privacy and security as major concerns.7 These opponents pose legitimate questions: Who will safeguard and maintain EHRs? Who may access them?8 In addition, making a patient’s records available in electronic form potentially exposes confidential health information to a host of indirect uses, “such as research, analysis, public reporting, provider certification and accreditation, and marketing and other commercial activity.”9

4. See id.
6. Obama Pledges, supra note 5.
7. Miller, supra note 5, at 353.
8. See id.
Even some physicians oppose digitizing their patients’ health records. These healthcare providers see computerized records systems as “black boxes,” and they worry that losing control over the system will force them to rely on computer technology experts who do not fully appreciate the need for privacy in the medical profession. To opponents of digitizing health records, President Obama’s pledge forces the American public to choose technological advancement over personal privacy.

Putting economics aside, the real debate over electronic health records can be summed up in a single question: Are electronic health records and patient privacy mutually exclusive? This Note argues that EHRs and patient privacy are compatible and may peacefully coexist. Ultimately, this Note will conclude that a shift to digital health records in the United States can promote efficiency, patient care, and safety, while at the same time respecting patient privacy and personal security. To reach this conclusion, a number of political, legal, and policy considerations require evaluation. Part I of this Note will discuss the background of EHRs and the origin of the debate over them. In addition, Part I will discuss federal and state privacy legislation, particularly the Health Insurance Portability and Accountability Act, which governs patient privacy in the medical realm. Part II will analyze the debate over EHRs and patient privacy, considering both the benefits and detriments of each approach. Part III will attempt to reconcile the competing camps. Finally, Part IV will conclude by offering a prognosis that EHRs and patient privacy can survive side-by-side.

I. EXPLORING A NEW MEDICAL CHART: ELECTRONIC HEALTH RECORDS

A. What is an Electronic Health Record?

A common definition of Electronic Health Records comes from the Health Information Management Systems Society (HIMSS). According to HIMSS:

The Electronic Health Record (EHR) is a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. Included

---

11. Id.
12. See Miller, supra note 5, at 354.
in this information are patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data, and radiology reports. The EHR automates and streamlines the clinician’s workflow. The EHR has the ability to generate a complete record of a clinical patient encounter, as well as supporting other care-related activities directly or indirectly via interface—including evidence-based decision support, quality management, and outcomes reporting.\textsuperscript{14}

An EHR is created and maintained within an institution, such as a hospital, integrated delivery network, clinic, or doctor’s office.\textsuperscript{15} In some instances, insurance companies and other third-party payers also keep EHRs for current and future reference.\textsuperscript{16} Notably, EHRs differ from personal health records, known as PHRs.\textsuperscript{17} EHRs comply with the Health Insurance Portability and Accountability Act (HIPAA), and only healthcare professionals can maintain and modify them.\textsuperscript{18} In contrast, a PHR is not HIPAA-compliant and the patient, not a health care professional or institution, controls all of the information it contains.\textsuperscript{19}

EHRs exist in two primary forms: Older records, typically recorded before 2000, have been scanned and stored as a graphic file; newer records, typically recorded after 2000, have been electronically created.\textsuperscript{20} The difference often turns on whether health care professionals wrote the initial information in the record by hand.\textsuperscript{21} The United States Government has defined four key features of a complete EHR system: computerized orders for prescriptions; computerized orders for tests; reported test results; and physician notes.\textsuperscript{22}

\textbf{B. Medical Records}

Hippocrates, known as the “father of Western medicine,”\textsuperscript{23} created the first health record.\textsuperscript{24} Hippocrates believed that a medical
record should reflect the course of disease and indicate its probable cause.\textsuperscript{25} According to the National Institutes of Health National Center for Research Resources, while Hippocrates’ goals for medical records remain valuable, new times and new technology demand new goals for patients’ medical records.\textsuperscript{26} Now, more than two thousand years later, science, research, and technology have afforded health care professionals the ability to provide patients with vastly more information about their health, all of which requires documentation in an accurate, secure fashion.

Despite recent media attention, EHRs are not a new technology.\textsuperscript{27} Leaders in the industry began writing computer programs that would house and retrieve patients’ health records as early as 1958.\textsuperscript{28} According to one study, “by 1965 . . . at least 73 hospitals and clinical information projects and 28 projects for storage and retrieval of medical documents and other clinically-relevant information were underway.”\textsuperscript{29} Much of the technology for EHRs came from work done at academic medical centers.\textsuperscript{30}

In their first decade of use, EHRs showed improvements in patient care, which generated much excitement among information technologists in controlled trials.\textsuperscript{31} However, many of these early projects “had significant technical and programmatic issues, including non-standard vocabularies and system interfaces.”\textsuperscript{32} One study indicates that, as of 2009, only about 8% of the nation’s 5,000 hospitals and 17% of its 800,000 physicians used an electronic record-keeping program that the Obama administration anticipates implementing in the next five years.\textsuperscript{33}
As for their place on the political agenda, EHRs came to the forefront at the beginning of the Clinton Administration. One of President Clinton’s primary goals was to improve the American health care system. Not only did the President aim to strengthen the United States’ Medicare and Medicaid systems, improve the quality of patient care, and increase the accessibility of health care for more Americans, he also intended to streamline the health care system by endorsing the shift to EHRs for all areas of medical personnel. Despite this, the President recognized the potential adverse consequences of their implementation. Thus, his administration promulgated innovative federal regulations safeguarding the privacy of EHRs, and Clinton himself issued an executive memorandum order preventing genetic discrimination in the hiring and promotion of federal employees.

Succeeding the Clinton Administration in 2001, President George W. Bush inherited the campaign for EHRs. In 2005, Bush called upon doctors and other health care personnel to eliminate paper records entirely. In an effort to reign in the already spiraling cost of American health care, President Bush stated that EHRs had the potential to “help change medicine and save money and save lives.” While the Bush Administration advocated for the shift to EHRs, it failed to implement an entirely electronic system. Presumably, the shift to EHRs will continue to unfold throughout President Obama’s term in office.

C. Privacy Regulations and the Health Insurance Portability and Accountability Act

1. Introduction to Privacy Regulations

The federal government has frequently assembled taskforces, drafted legislation, and instituted mechanisms to protect the privacy and security of individual health records. In the past four decades,
the federal government has expressed increasing concern for the protection of electronically stored and transmitted health records. In 1973, under President Richard Nixon, the U.S. Department of Health, Education, and Welfare commissioned the Advisory Committee on Automated Personal Data Systems to evaluate the impact of computerized record keeping. During the Committee’s tenure, it developed the Code of Fair Information Practice, which outlined five key principles for addressing the security of digital health records: openness, disclosure, secondary use, correction, and security.

The federal government continued its efforts to pass legislation regarding patient privacy and security throughout the remainder of the twentieth century. In 1974, Congress passed the Privacy Act, which protects certain personal information held by federal agencies. Additionally, the United States joined the Organization for Economic Cooperation and Development, which published the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980. Eight years later, the Federal Trade Commission entered the electronic data protection arena by publishing Privacy Online: A Report to Congress, which recommended effective self-regulation as the “preferred approach to protecting individuals’ privacy.” Federal involvement in privacy regulation culminated in 1996 with the passage of a comprehensive health information privacy framework—the Health Insurance Portability and Accountability Act.

2. An Overview of HIPAA

In 1996, under the leadership of President Clinton, Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The legislative history of HIPAA lists five primary purposes of the law: improving portability and continuity of health insurance coverage in the group and individual markets; combating waste, fraud, and abuse in health insurance and health care delivery; promoting the use of medical savings accounts; improving access to


41. Id. at 2.
42. Id. at 1—2.
43. Id. at 2.
44. Id.
45. Id.
46. Id.
47. Id.
long-term care services and coverage; and simplifying the administration of health insurance.\footnote{49} While the preamble sets out the initial purposes of HIPAA, the Act’s Administrative Simplification provisions regulate medical records (including EHRs), privacy requirements, and security standards for health care transactions.\footnote{50} Title II of HIPAA sets out a number of health care offenses and creates programs intended to combat healthcare fraud and abuse.\footnote{51} For purposes of this Note, the most important parts of Title II are the Administrative Simplification provisions of HIPAA, set forth in \S\ 261 through \S\ 264.\footnote{52}

HIPAA’s Administrative Simplification provisions task the Department of Health and Human Services (HHS) with creating rules to increase the health care system’s efficiency by creating standards for using and distributing health care information.\footnote{53} According to the Act, Congress intended the Administrative Simplification provisions to improve “the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.”\footnote{54}

Parts of the Administrative Simplification provisions were meant to bring health care and health maintenance to the digital age. Congress sought to decrease administrative costs by “establishing uniform standards of electronic payment-related health care transactions.”\footnote{55} Section 262 of HIPAA amended the Social Security Act by tasking HHS with recommending standards for: (1) electronic transactions, as well as the data elements for such transactions; (2) a unique health identifier for each individual, employer, health plan, and health care provider; and (3) code sets for appropriate data elements for the transactions.\footnote{56} In response to this initiative, Congress enacted the Administrative Simplification Compliance Act of 2001, allowing covered entities one additional year to comply with the standards, provided that they file a compliance plan with HHS.\footnote{57} In

\footnote{49} John Casillas, \textit{A Summary of HIPAA’s Administrative Regulations}, in \textit{TREATISE ON HEALTH CARE LAW} \S\ 8A8.syn (2010); see also id.
\footnote{50} Casillas, \textit{supra} note 49.
\footnote{51} See \S\S\ 201—250, 110 Stat. at 1992—2021.
\footnote{52} \S\S\ 261—264, 110 Stat. at 2021—34; Susan Godstone, \textit{Health Insurance Portability and Accountability Act}, in \textit{TREATISE ON HEALTH CARE LAW} \S\ 13.01 (2010).
\footnote{53} Godstone, \textit{supra} note 52.
\footnote{54} \textit{Id.}; see \S\S\ 261—264, 110 Stat. at 2021—34.
\footnote{55} Godstone, \textit{supra} note 52.
\footnote{56} \textit{Id.}
the Act, Congress also provided that these standards apply to transactions such as: health care claim or equivalent encounters; eligibility for health plans; referral certification and authorizations; health care claims status; and health plan enrollments and disenrollments. In addition to setting national standards for electronic health care transactions, HHS also addressed security and privacy concerns regarding health care data.

3. The HIPAA Privacy Rule

HHS scheduled the Privacy Rule, part of the Administrative Simplification provisions of HIPAA, for implementation in April of 2001, mandating compliance and implementation for covered entities by April of 2003. Codified at 45 C.F.R. § 160—164, the rule went into effect on August 14, 2002. According to HHS, the HIPAA Privacy Rule:

- establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

“Protected health information” means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other media. Given the diversity of the “health care marketplace,” HHS implemented this “flexible and comprehensive” Rule to account for the many purposes the agency sought to address. Whom the Privacy Rule and Administrative Simplification provisions govern is significant from a compliance perspective. HIPAA categorizes as ‘covered entities’ those subject to the Privacy Rule. This definition includes health plans, health care clearing

58. Godstone, supra note 52.
59. Id.
60. Casillas, supra note 49.
61. Godstone, supra note 52.
63. 45 C.F.R. § 160.103 (2010).
65. Id.
houses, and any health care providers who transmit information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA.66

The Privacy Rule covers a very specific form of health data, known as “protected health information,” which is any individually identifiable health information “held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.”67 In turn, HIPAA defines “individually identifiable health information” as:

information, including demographic data, that pertains 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.68

Examples of identifiers include an individual’s name, address, birth date, and social security number.69

The Privacy Rule determines when a covered entity may use or disclose an individual’s protected health information. According to the Rule, a covered entity may not use or disclose protected health information except under the following two circumstances: (1) when the Privacy Rule so permits or requires; or (2) as the individual or the individual’s personal representative authorizes the use or disclosure in writing.70 Aside from the required disclosure of protected health information, a covered entity is permitted to use or disclose protected health information in the following situations: “(1) to the individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and, (6) Limited Data Set for the purposes of research, public health or health care operations.”71

In addition to the Privacy Rule, the Administrative Simplification provisions also required HSS to adopt standards to ensure the security of electronic protected health information.72 The Security Rule promulgated by HHS requires covered entities to adopt administrative, physical, and technical measures to protect the

66. Id. at 2—3.
67. Id. at 3.
68. Id. at 4.
69. Id.
70. Id.
71. Id. at 4—5.
72. Godstone, supra note 53.
confidentiality, integrity, and availability of this information.\textsuperscript{73} Under the Security Rule, HHS standards help protect personal health information and the use of electronic signatures by covered entities.\textsuperscript{74} This rule largely accounts for the backlash against the HIPAA regulations in the 1990s and early 2000s, because of its perceived cost of compliance.\textsuperscript{75} For the most part, analysts have agreed with this assessment, finding that “the IT/IS infrastructure in the medical complex was never constructed to meet the ‘defense system standards’ of security that are proposed in the regulations.”\textsuperscript{76} Nevertheless, the Security Rule within HIPAA does “set forth minimum standards for the physical, hardware, and software infrastructure used in conjunction with storing, transmitting and/or otherwise managing protected health information.”\textsuperscript{77}

4. HIPAA and EHRs

Since their entrance into the medical documentation field, EHRs have raised great concern about their potential misuse. In 2009, Congress began linking federal stimulus money for EHRs to improved privacy and security rules under HIPAA.\textsuperscript{78} Congress recognized, for the first time, that for physicians, hospitals, and the medical industry in general to switch from paper to electronic health records, it must create new enforcement mechanisms for ensuring the records’ privacy and security.\textsuperscript{79} In 2009, Congress introduced the American Recovery and Reinvestment Act (ARRA), codifying a new approach to ensure the privacy and security of EHRs.\textsuperscript{80} Under the ARRA, physicians and hospitals that become “meaningful users” of health information technology will be paid incentives beginning in 2011.\textsuperscript{81} In addition, the Health Information Technology for Economic and Clinical Health Act, codified in Title XIII of the ARRA, creates substantial changes to the HIPAA privacy and security rules.\textsuperscript{82} According to HHS, the technologies and methodologies proposed in the amendments to HIPAA are meant to render protected health

\textsuperscript{73} Id.
\textsuperscript{74} Casillas, supra note 49.
\textsuperscript{75} Id.
\textsuperscript{76} Id.
\textsuperscript{77} Id.
\textsuperscript{79} See id.
\textsuperscript{81} Wilder, supra note 78.
\textsuperscript{82} Id.; see §§ 13400—13411, 123 Stat. at 258—76.
information in an electronic form “unusable, unreadable, or indecipherable to unauthorized individuals.”

In addition, the new HIPAA rules contain a security breach notification provision, which requires that individuals receive notice if their protected health information has been disclosed. Assuming that the Obama Administration enforces HIPAA more vigorously than the Bush Administration, the new rules will impose a more stringent penalty on hospitals or physicians that allow breaches of confidentiality, as well as the individuals or entities that wrongfully acquire or use an individual’s protected health information.

For instance, the HIPAA enforcement amendments create a new tiered penalty structure, with fines ranging from as little as $25,000 to as much as $1.5 million. Furthermore, these amendments provide for greater communication among state attorneys general to enforce HIPAA rules and investigate the intent of violators. To safeguard against the greatest threat to protected health information—misuse by employees—the new amendments allow prosecutors to bring criminal charges against employees who wrongfully access an individual’s protected health information.

The new approach to HIPAA has also resulted in a change in the agency tasked with enforcing the Act. As of August 3, 2009, Congress delegated the administration and enforcement of HIPAA to the Department of Health and Human Services’ Office for Civil Rights. Previously, the Centers for Medicare and Medicaid Services handled all HIPAA matters. This shift between agencies not only consolidates enforcement, eliminates duplication, and increases the efficiency of department efforts to protect health information privacy, but it also acknowledges that “[s]ecurity and privacy of health information are increasingly intersecting as the Department [of Health and Human Services] works with the health industry to adopt electronic health records and participate in an even greater level of electronic exchange of health information.”

83.  Wilder, supra note 78.
84.  Id.; see § 13402, 123 Stat. at 260—63 (“A covered entity . . . shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been . . . disclosed as a result of such breach.”).
85.  Wilder, supra note 78.
86.  Id.; see § 13410(d), 123 Stat. at 272—74.
87.  See § 13410(e), 123 Stat. at 274—75; Wilder, supra note 78.
88.  Wilder, supra note 78.
90.  Id.
91.  Id.
92.  Id. (internal quotation marks omitted).
Many have projected that although the Bush Administration brought few HIPAA enforcement actions, their frequency will likely increase in the years to come. The Office of Civil Rights will probably receive greater authority to pursue HIPAA violations, as well as greater resources to enable their pursuit. In conjunction with the Health Insurance Technology for Economic and Clinical Health Act (HITECH), healthcare lawyers predict that enforcement activity will immediately increase, and thus physicians and hospitals should prioritize the protection of EHRs.

States have recently followed the lead of the federal government by more strictly enforcing their own laws against health record privacy infringements. For instance, on July 16, 2009, the California Department of Public Health fined Kaiser Permanente Hospital $187,500 for patient privacy violations. The Department found that the hospital, located in Los Angeles County, compromised the privacy of four patients when several employees improperly accessed those patients’ electronic health records. This penalty followed another fine against the same hospital, just two months earlier, for improper access to the medical records of Nadya Suleman, popularly known as “Octomom.”

Upon discovering the breach of patients’ EHRs, the Department not only issued Kaiser Permanente a heavy fine, but also gave the hospital ten days to create and implement a plan of correction for future breaches. This case highlights not only the real risk of unlawful access to EHRs, but also the increasingly punitive response of federal and state governments to these breaches. During the first five months of mandatory self-disclosure, health organizations reported an alarming 823 breaches of individuals’ protected health information to the California Department of Public Health alone.

Other states have also recently enacted legislation to complement federal HIPAA laws and to better protected the privacy of patient records. In April of 2009, New Mexico Governor Bill Richardson signed Senate Bill 278, which created an EHR system for

93. See, e.g., id.
94. Id.
95. Id.
97. Id.
98. Id.
99. Id.
100. Id.
101. Id.
the entire state of New Mexico. According to Richardson, the rising popularity of EHRs required an integrated and uniform system. As an additional privacy measure, the bill requires patients to consent annually to have their health information made electronic. Furthermore, the New Mexico bill clarifies the rights of individuals regarding disclosure of information contained within their EHRs.

II. A HEALTHY DEBATE: EXALTING ACCESS OR PRAISING PRIVACY?

A. The Problem of Privacy: The Case Against EHRs.

Opponents of EHRs have articulated several concerns with regard to privacy issues. First, since an EHR “can be called up instantaneously by someone with access to the data system,” the opponents of EHRs argue that there is a greater threat of improper access and distribution with electronic, rather than with paper, records. While these opponents acknowledge that paper health records may be photocopied or faxed, they claim that widely distributing paper records is more difficult and requires physical possession. These computerized records systems are sometimes likened to “black boxes,” and health professionals claim such a design threatens their autonomy over the system.

Second, critics worry about proposals to “link all medical records systems so that patient data can be accessed wherever and whenever patients require medical services.” The concern is that an individual’s access to a minute portion of one record may open that individual’s access to any other portion of the patient’s medical records. For example, suppose an employer obtains access to an employee’s records from the employee’s recent physical with the company’s doctor, because the company has recently implemented a benefits program in which employees who lose ten pounds, quit smoking, or lower their blood pressure have the chance to gain financially or in some other way. Under some EHR systems, the
employer’s access to the records from the employee’s recent physical may concurrently grant the employer access to all the other health records of that employee. Suppose the employer had a wandering eye and chose to access the employee’s medical records from a gynecological examination. If the employer were to find out that the employee tested positive for an STD, contracted cervical cancer, or was pregnant, that information may affect the employee’s position at her job. This is precisely the kind of misuse that opponents of EHRs fear is in our immediate future.

Third, critics warn that insurance companies will have too much access to patient information in the managed care context. Historically, the medical profession has operated on a fee-for-service basis. Under a fee-for-service regime, physicians or other healthcare professionals produce—and retain—a patient’s records, and a patient’s insurance company is only afforded access to particular records as needed for insurance claim review. Although HIPAA created a system in which disclosure of medical records requires patient authorization, most patients grant permission in a “blanket fashion.”

The contrast between fee-for-service and managed-care medical record handling is striking. In the managed care context, the provider of care and the insurer are, in effect, one and the same. Therefore, any medical information held by the provider of medical care, such as the physician, is likewise held by the entity paying for the care, namely the insurer. The concern, then, is that the insurer will access patient records and view potentially detrimental health information that a physician and patient would otherwise not provide to an insurer, at least not in a fee-for-service context. Patients fear that insurers (via health maintenance organizations) will gain access to far more information than they could have in the past, and thus disadvantage patients by restricting payment for their medical care or limiting the plans available to purchase.

Fourth, opponents of the shift to EHRs voice concerns about the cost of making the switch. All involved agree that cost poses a

114. Id.
115. Id.
116. Id.
117. Id.
118. Id.
119. Id.
major obstacle to this technological innovation. Experts concur that physicians, hospitals, and other medical care providers need “new models of delivery and easier-to-use technology to reduce the expense and technical headaches” that come with this new technology. Companies such as General Electric, I.B.M., Verizon, and Dell are already vying for a competitive edge in the market for EHR software, promising that faster network connections and less expensive computers will make the transition to digital health records less burdensome. However, opponents of the shift to EHRs rightfully raise the question of just how certain the government can be about the success and streamlining effect of digital health records. Potentially, “physicians [will] buy lots of computer hardware and software, but see no improvements, leaving a legacy of wasted money, angry doctors and disrupted care for patients.”

Finally, opponents of EHRs worry about an increased risk of medical identity theft. This alarming phenomenon can take on a variety of forms, such as stolen Social security numbers or basic member identification and group policy numbers found on insurance cards. However, the most common cases occur when company insiders, such as information technology personnel or staff nurses, steal such information. An insider in the medical office may “download vital personal insurance data and related information from the operation’s computerized medical records, then sell it on the black market or use it [herself] to make fraudulent billing claims.”

For example, a highly publicized case of medical identity theft occurred in Weston, Florida at a Cleveland Clinic branch office in 2006, when an office clerk downloaded more than 1,100 Medicare patients’ medical records and gave them to a family member, who made a $2.8 million profit from false claims. Furthermore, a report issued by the federal government in 2007 indicated that each year more than 250,000 Americans are victims to medical identity theft. It is widely believed that this number has already risen—and will continue to rise—due to the massive shift to EHRs, which makes it

121. Id.
122. Id.
123. Id.
125. Id.
126. Id.
127. Id.
128. Id.
even easier for medical identity thieves to complete their operations.\textsuperscript{129} Thus, health information privacy activists campaign against the shift to EHRs, fearing that President Obama has planned to spend $20 billion to increase their prevalence across the nation without yet implementing the needed “aggressive safeguards.”\textsuperscript{130} Without these protective measures in place, they fear that the government is “building an infrastructure for massive medical fraud.”\textsuperscript{131}

\textbf{B. Protecting Privacy: The Case Against the Case Against EHRs}

Despite the difficulty of policing medical records, a number of meaningful measures do exist.\textsuperscript{132} Lisa Gallagher, the Senior Director of Privacy and Security for the Healthcare Information and Management Systems (HIMSS), claims that despite the 2002 HIPAA amendments that relaxed privacy standards for medical records, medical privacy regulations are baring “new teeth.”\textsuperscript{133} As mentioned above, the same amendments now provide criminal penalties, civil fines as high as $1.5 million, and up to ten years in prison for violations of patient privacy via improper use or access to patient medical records.\textsuperscript{134} Furthermore, HIPAA now mandates that providers must enable patients to have access to their medical records in digital form.\textsuperscript{135}

Money also provides an incentive for hospitals, physicians, and hospital staff members to comply with privacy protocols. The American Recovery and Reinvestment Act (ARRA) of 2009, which provides for much of the federal financing for the shift to EHRs, offers “financial incentives for healthcare businesses to meet its privacy guidelines, and punishment for people and businesses that fail.”\textsuperscript{136} For example, under ARRA, an individual doctor may claim $44,000 for implementing health information technology (IT) between 2011 and 2015 that meet federal privacy and security standards.\textsuperscript{137} Likewise,

\textsuperscript{129} \textit{Id.}
\textsuperscript{130} \textit{Id.}
\textsuperscript{131} \textit{Id.} (internal quotation marks omitted).
\textsuperscript{133} \textit{Id.}
\textsuperscript{135} \textit{Can Electronic Medical Records Be Secured?, supra note 132.}
\textsuperscript{136} \textit{Id.}
\textsuperscript{137} \textit{Id.}
an individual hospital may claim $2 million during those years for
health IT implementations that meet the same federal privacy and
security standards.\textsuperscript{138} In contrast, any individuals or organizations,
such as doctors or hospitals, that fail to comply with the ARRA privacy
and security standards get nothing.\textsuperscript{139} This promise of hefty financial
gain for privacy and security compliance will presumably incentivize
hospitals, physicians, and other medical personnel to comply with
HIPAA privacy guidelines as they pertain to EHRs.

Furthermore, the ARRA regulations encourage a zero-tolerance
policy intended to deter patient privacy breaches.\textsuperscript{140} According to
John Halamka, the Chief Information Officer of Harvard Medical
School, authorized individuals who wrongfully access individual
patient records may be automatically terminated and face criminal
charges as well as civil fines under the ARRA regulations.\textsuperscript{141}
Moreover, if a health care institution allows the breach of more than
500 medical records, then it must notify “prominent” media in the
region of the breach.\textsuperscript{142} Obviously, no medical provider wants to
advertise its privacy breaches in the \textit{New York Times}. This new
regulation encourages physicians and hospital personnel to think
twice before improperly accessing patients’ EHRs.

Moreover, the following technical safeguards exist to protect
against privacy breaches of patient EHRs, such as:

unique patient and access identifiers; ‘audit trails,’ which are electronic methods of
detecting and recording the identities of anyone who accesses a record; encryption of
external transmissions or record information; appointment of internal information
security officers with responsibility to police record-keeping practices; and ‘firewalls,’
which are electronic barriers that isolate records systems from unauthorized access or
penetration.\textsuperscript{143}

Additionally, the Office of the National Coordinator for Health
Information Technology (ONC) may help protect personal health
records. On December 15, 2008 the ONC released a pivotal document
in EHR privacy, “Nationwide Privacy and Security Framework
Electronic Exchange of Individually Identified Health Information.”\textsuperscript{144}
The relatively short document articulates eight principles aimed at
tackling privacy and security challenges that arise from EHRs:\textsuperscript{145}
individual access, means for correction, openness and transparency, individual choice, data quality and integrity, safeguards, accountability, and collection, use and disclosure limitation. Most notably, the principles establish a uniform, consistent approach intended to address the privacy and security challenges related to EHRs, independent of any specific institution or legal paradigm. According to the ONC report, an important reason to adopt privacy and security protections is to build up the “public trust” needed to effectively communicate health information for the benefit of the patients. Implementing these principles would provide a universal platform on which to erect a robust infrastructure for protected medical data.

The accountability principle warrants particular attention. The report suggests that, at a minimum, mechanisms for ensuring privacy and security of medical records should include:

1. monitoring for internal compliance including authentication and authorizations for access to or disclosure of individually identifiable health information;
2. the ability to receive and act on complaints, including taking corrective measures; and
3. the provision of reasonable mitigation measures, including notice to individuals of privacy violations or security breaches that pose substantial risk of harm to such individuals.

The adoption of these principles would hopefully allow doctors, hospitals, and other health care providers to “follow a common approach to privacy and security and develop appropriate and comparable protections for information, thereby increasing trust in electronic exchange of individually identifiable health information.”

III. A PRESCRIPTION FOR PRIVACY

Digitizing health records is no longer an idea for the future. As evidenced by this Note, the transition from paper to electronic health records has been a long time coming in the United States, and President Obama has made it clear that as part of his health care reform agenda, patients’ health records will become digitized by 2014. This change, however, brings with it potentially serious consequences, and the United States government must work hand-in-hand with hospitals, physicians, and other health care professionals to ensure that patient privacy remains intact. A number of mechanisms

146. Id.
147. Id. at 1.
148. Id. at 6.
149. Id.
150. Id. at 9—10.
151. Id. at 5.
should be implemented in the next few years to accomplish this shift to digital health records. If these safeguards are observed, patient privacy and electronic health records may peacefully coexist.

First, the government should mandate a national “opt in” program for electronic health records. One of the best ways to maintain privacy and security is for individual patients to exercise control over their own health records. For instance, in an “opt in” system, patients would have to consent to the transfer of any electronic health information, aside from a general carve out (such as that in HIPAA) for routine needs. In effect, this would require physicians and health care providers to obtain informed consent from patients prior to digitizing their health records. In contrast, in an “opt out” system, patients would receive notice that their health information could be digitally transferred to a wide variety of healthcare providers, unless they signed a form prohibiting such transfers. The “opt in” system, therefore, provides a better safeguard to patient privacy, because it ensures that informed consent precedes the digital distribution of any health information.

Second, if the federal government determines that a national “opt in” system for EHRs is infeasible, patients should at least enjoy the right to flag certain health information (such as particular doctor’s visits) as confidential. This flagging system would ensure that patients could keep particularly sensitive information away from the broad network of providers that could otherwise access the electronic health record.

Third, hospitals, doctors, and other healthcare providers who intend to implement electronic health records systems should carefully train physicians and staff members on the hospital’s specific electronic health record system. In doing so, the hospital should emphasize “good practices” that respect patient privacy, as well as the possible financial and legal sanctions that may result from breaches of patient privacy. These standard training sessions could serve to remind physicians and hospital personnel that when it comes to patient privacy breaches, they have “skin in the game.”

Fourth, the federal government should implement technological safeguards ensuring the protection and privacy of information in EHRs. In 2000, the National Research Council

155. See id. at 702.
156. See id. at 702—03.
advocated that the federal government include new technological features to better protect Internet users’ privacy and anonymity.\textsuperscript{157} Technology safeguards could include electronic passwords, digital signatures, firewalls, time stamps, and other privacy protection software.\textsuperscript{158} With such safeguards and protective mechanisms in place, potential hackers will encounter great difficulty in even gaining access to health information, let alone misusing it.

IV. CONCLUSION

Tying federal funds to the implementation of EHRs via the ARRA ensures that EHR systems are here to stay. While great benefits will result from digitizing health records, great concerns for the protection of patient privacy will remain. Nevertheless, as this Note has attempted to show, patient privacy and electronic health records are not, in fact, mutually exclusive. While it may never be possible to ensure the absolute security of all records held in cyberspace, with the necessary safeguards in place, the government can at least assure the American people that their protected health information is receiving the highest feasible level of security. Working together, the government, healthcare providers, and patients can ensure that personal health information is protected long beyond 2014.

*Lauren Bair Jacques*

\textsuperscript{157} Keith A. Bauer, \textit{Privacy and Confidentiality in the Age of E-Medicine}, 12 \textit{J. Health Care L. \\& Pol'y} 47, 60 (2009).

\textsuperscript{158} \textit{Id.} at 60—61.

* Lauren Bair Jacques, J.D. Candidate 2011, Vanderbilt University Law School. B.A. Philosophy 2008, Vanderbilt University. The author would like to thank her husband, Richard, for his continuous support and encouragement throughout the creation of this Note.