Electronic Medical Records: How the Potential for Misuse Outweighs the Benefits of Transferability

Samuel J. Miller*

Introduction

Electronic medical records are touted by politicians as a way for the health care industry to save money while reducing errors in the treatment of patients.1 There are numerous benefits to electronic medical records: they allow for easier transfer of records between medical offices, may reduce the need for duplicative tests, and may signal to doctors when problems arise with patient care.2 Despite the benefits that electronic storage of medical records will bring, many people worry about the privacy and security of medical records.3 In fact, patients cite privacy and security concerns as their greatest concern with respect to electronic medical records.4 Cutting edge technologies used to store and transmit electronic medical records, such as the VeriMed microchip, a device that can be implanted in humans and allows medical providers to instantly obtain the patient’s medical information by scanning the microchip, may only exacerbate public

---

1 J.D. Candidate, Suffolk University Law School, 2009; B.A., summa cum laude, University of Massachusetts – Boston, 2006. Mr. Miller can be reached at sam.miller@hotmail.com.

2 See Michael Fletcher, President Promotes Switching To Electronic Medical Records; Bush Says Paperless System Would Cut Costs, Improve Care. WASH. POST, Jan. 28, 2005, at A7. President George W. Bush said on January 27, 2005, that electronic medical records can "help change medicine and save money and save lives." Id.


4 See Terry & Francis, supra note 3, at 696.
The government may be exercising a legitimate interest in maintaining public health when it seeks to utilize electronic medical records of patients, but what the government considers its interest in “public health” is ambiguous at best. The debate over the allowable use of medical records by the government can be characterized as a struggle between heads of executive agencies, seeking to acquire as much information as possible, and the public, seeking to confine the use of medical records to authorized use. Despite the government’s interest in obtaining the most information possible, the General Accounting Office reported in 2007 that the government had no cohesive strategy to ensure the privacy of electronic medical records, even as the government continues to encourage the use of electronic recordkeeping. While the government may need to utilize the electronic medical records of citizens in response to a public health crisis, such as a bioterrorism event, a strategy to protect personal privacy must be implemented. The transition to electronic medical records should not force Americans to choose between technological advancement and their historical right to privacy.

The government should not frame the debate over privacy in electronic medical records in a way that uses the fear of terrorism to force people to choose between privacy issues

---

5 See VeriChip Corporation, Intro to VeriMed FAQ, http://www.verimedinfo.com/faq.asp (last visited Nov. 4, 2008). “The VeriMed microchip contains a unique 16-digit VeriMed number. This number enables healthcare professionals to obtain your vital medical information through a highly secure online database. No other information is contained on the microchip for privacy reasons.” Id.

6 See Wendy K. Mariner, Mission Creep: Public Health Surveillance and Public Policy, 87 B.U. L. Rev. 347, 384 (2007). “Courts either fail to specify what they mean by public health, or seem to have an understanding that is different from what is intended by public health agencies. While a judge may be thinking of outbreak investigation, public health agencies may have in mind the longer-term goal of using data in a research study to find a cure for cancer.” Id.

7 See Lawrence O. Gostin, When Terrorism Threatens Health: How Far Are Limitations on Personal and Economic Liberties Justified?, 55 Fla. L. Rev. 1105, 1162 (2003). Gostin notes that “[p]ublic health policy is riddled with contradictions. Agency officials seek power without constraint...The liberal public, on the other hand, prefers strict limits on agency action.” Id.

8 Robert Pear, Warnings Over Privacy of U.S. Health Network, N.Y. Times, February 18, 2007, at A22 (reporting that the General Accounting Office stated that the Bush administration had “a jumble of studies and vague policy statements but no overall strategy” and that privacy protections would be included in networks linking health care providers).

9 See Gostin, supra note 7, at 1130 (arguing that there is no public health infrastructure currently in place in the event of a bioterror attack).

10 See Paul Starr, Health and the Right to Privacy, 25 Am. J. L. & Med. 193, 194 (1999) (stating “the right of privacy must be judiciously balanced against other values in finding the appropriate policy”).
and public safety.\textsuperscript{11}

In Part I, this note will focus on the history of privacy regarding medical records, focusing on government proposals and court decisions that defined the scope of the government's control over medical records. Part II will look at current actions by governments and private companies with respect to creating large databases of medical records. In Part III, this note will consider the problems that arise from allowing the government unfettered access to medical records, how it affects patient safety, and how it can be misused even in times of emergency.

Since the beginning of the electronic age, the compiling of medical records in computerized databases has caused people to question what a health care provider or government agency could do with the data.\textsuperscript{12} In the last quarter of the 20th century there was a proliferation of issues with respect to the privacy of medical records.\textsuperscript{13} The right to control and access one's own medical record is widely considered a patient's right and the patient can almost universally get access to their own medical record.\textsuperscript{14} Courts have recognized that individuals have a privacy right pertaining to their medical records.\textsuperscript{15} However, the privacy rights of individuals have been eroded by passage of

\begin{flushleft}
11 See Peter P. Swire & Lauren B. Steinfeld, Modern Studies in Privacy Law: National Health Information Privacy Regulations Under HIPAA: Security and Privacy after September 11: The Health Care Example, 86 MINN L. REV. 1515, 1515-16 (2002). The authors note that in the aftermath of the September 11, 2001, terrorist attacks Wall Street Journal polls showed that, for most people, concerns about public safety exceeded concerns about privacy issues, whereas before the September 11, 2001, terrorist attacks, loss of privacy was the highest ranking concern. \textit{Id.} The implication is that, when faced with the fear of terrorism, the public will choose security over privacy. \textit{Id.}
\end{flushleft}

\begin{flushleft}
\end{flushleft}

Each of these data areas poses different privacy questions, involving different tradeoffs between the privacy interests of the individual data subject and the social or organizational interest in the free flow of patient records. Medical data poses this efficiency-privacy dilemma in a particularly acute form: for the great majority of people, records of physical or mental illness are the more sensitive kinds of personal information that will ever be systematically collected, yet widespread access to medical records is vitally important in treatment, in research, in the formation of public policy, and in compensating the victim of accident or disease.

\textit{Id.}

\begin{flushleft}
\end{flushleft}

\begin{flushleft}
\end{flushleft}

\begin{flushleft}
15 See Doe v. City of New York, 15 F.3d 264, 267 (2nd Cir. 1994) (extending the right of
the Model State Emergency Health Powers Act, and movements by the Executive
Branch of government to create databases of medical records ostensibly for ease of
medical case, and creation by municipalities of databases listing everyone with certain
diseases.16

I. History of Medical Records Privacy

Court Decisions on Medical Records Privacy

The Constitution has not been interpreted as granting strong information
privacy protections to individuals.17 The government is allowed access to patient
medical records, subject only to a test that balances the governmental invasion of
privacy against the strength of the government's interest in accessing the data.18 In
Whelan v. Roe,19 the Supreme Court found that a New York statute that allowed the state
to control medical records related to prescribing of medicine by doctors in a centralized
database for five years was not unconstitutional.20 The Court understood that allowing
the state access to large quantities of records was essential in order for the government
to provide a wide range of public services.21 The Court also noted that the state has an

16 See generally MODEL STATE EMERGENCY HEALTH POWERS ACT (Center for Law and the
Public's Health at Georgetown & Johns Hopkins Universities 2001) [hereinafter MSEHPA],
See Minor, infra note 30; see also Krent, et al., infra note 64.
17 Starr, supra note 10, at 194 (stating “[p]rivacy is not an all-purpose trump card; it is not the only
value implicated in the rules governing the control of information.”).
18 See Lawrence O. Gostin et al., Balancing Communal Goods and Personal Privacy Under a National
Health Informational Privacy Rule, 46 ST. LOUIS U. L.J. 5, 12 (2002) (stating that “courts have
employed a flexible test balancing the government invasion of privacy against the strength of the
government interest”).
20 See id. at 603-04. The statute upheld was the New York State Controlled Substances Act. NY
CLS Pub Health § 3300 (2007). The statute classified drugs into five different schedules and
required doctors who prescribed Schedule II drugs to use an official state form for the
prescription. Id. at 592. “Schedule I” was highly dangerous and abused drugs which had no
legitimate medical purpose. Id. “Schedule II” was where the most dangerous of the drugs that
had a legitimate medical purpose were classified, and included cocaine, methadone, and
amphetamines. Id. at 592-93, 593 n.8. Doctors prescribing Schedule II drugs had to list the
prescribing doctor, the pharmacy, the drug, and the name, address, and age of the patient. Id. at
593. A copy of this information was provided to the New York State Department of Health. Id.
21 See id. at 605 (“The collection of taxes, the distribution of welfare and social security benefits,
the supervision of public health, the direction of our Armed Forces, and the enforcement of the
criminal laws all require the orderly preservation of great quantities of information, much of
interest in using "new techniques for control" with respect to impeding the spread of "dangerous drugs." However, the court recognized that citizens have a simultaneous interest in keeping their medical records private.

In United States v. Westinghouse Electric Corp. (Westinghouse II) the Third Circuit restricted when the government could get access to medical records, recognizing that medical records were of a different nature than other personally identifiable files. The lower court had previously ruled that doctors from the National Institute for Occupational Safety and Health could get access to employee medical records in order to investigate whether employees were being exposed to harmful materials while working. The Westinghouse II court stated that medical records were of a different character than other records because medical records pertain to one's physical body. The Westinghouse II court declared that there were factors relating to the type of record and the potential harm of its release to be considered in deciding between the competing interests of the individual and the government in releasing personal medical information. The Third Circuit allowed the National Institute for Occupational Safety
and Health access to medical records of the employees of Westinghouse, subject to the employees' informed consent.  

II. Government and Private Industry Actions

Government Movements on Medical Records

President William J. Clinton, as part of his initial push to reform the health care industry upon his inauguration in 1993, included as part of his proposal a health identification card, called a Health Security Card, that would allow patients to carry their medical records at all times. The Health Security Card was to identify the holder and to bring together information and medical data from different health databases, with the stated purpose of minimizing health care administrative expenses. The National Health Act, the legislation that would have created the Health Security Card, did not specify what type of information was to be on the card, leaving that to the National Health Board, an entity created by the National Health Act. A presumption in the early 1990s, when the National Health Act proposed the Health Security Card, was that the card would not contain much information about the person because of limitations on how much a credit card sized card could contain. While many welcomed the idea of a Health Security Card, many privacy rights advocates were alarmed by the proposal for a Health Security Card. However, Clinton's Health Security Act was not enacted into law and the Health Security Card was never created.

need for access' - meaning, a recognizable public interest.” Gostin et al., supra note 18, at 12 n.31.
29 See Gostin et al., supra note 18, at 12 n.31 (stating the five factors enumerated in Westinghouse II).
Today, the Second, Third, Fifth and Ninth Circuits have found a right of privacy for individuals not being forced to reveal personal information upon government request. See Fred H. Cate, The Changing Face of Privacy Protection in the European Union and the United States, 33 IND. L. REV. 174, 210 (1999); see also Westinghouse II.
31 Id. at 256. Minor notes that “[i]t would identify its holder as eligible for health benefits and could reveal an identification number. Second, the card would bring together patient information and medical data through a system of databases, minimizing administrative expenses.” Id.
32 Id. at 277.
33 Id. at 277 (stating, “Should the chosen card be an ATM-style card, only a small amount of data could be stored on the magnetic strip -- limited perhaps to name, date of birth, identification number and coverage details. The card would have no room for medical records.”). Id.
34 See Minor, supra note 30, at 278 (observing that while the Americans Civil Liberties Union was against the Health Security Card, many United States Senators were in favor).
35 See id. at 254 (noting that within one year after the Health Security Card was proposed, the
The Privacy Act of 1974 (Privacy Act), while not specific to medical records, gives citizens some control over the information that is collected about them by the federal government.\textsuperscript{36} The Privacy Act allows the government to store only relevant and necessary personal information, maintain accurate records, and implement safeguards that ensure the security of the information.\textsuperscript{37} The Privacy Act also grants individuals whose records are stored the right to review and copy the records.\textsuperscript{38} However, the Privacy Act applies only to federal agencies and entities contracting with the federal government.\textsuperscript{39} Hospitals in particular are not protected by the Privacy Act, and can be forced to turn over personal medical records to the government upon request or subpoena.\textsuperscript{40}

The Health Insurance Portability and Accountability Act (HIPAA) became law in 1996.\textsuperscript{41} While the act was not primarily an act that regulated the privacy of a patient's medical records, Congress did seek to establish rules to protect the privacy of patients' medical records.\textsuperscript{42} HIPAA required that those who transmit health records in electronic form adhere to safeguards to prevent the release of confidential patient data and ensure that employees of health providers follow guidelines to prevent inadvertent release of patient information.\textsuperscript{43} When HIPAA was passed in 1996, Congress had until 1999 to proposal was effectively withdrawn).


\textsuperscript{37} See Cate, \textit{supra} note 29, at 210. According to Cate, "[t]he federal Privacy Act obligates government agencies to store only relevant and necessary personal information; collect information to the extent possible for the data subject; maintain records with accuracy and completeness; and establish administrative and technical safeguards to protect the security of records." \textit{Id.}

\textsuperscript{38} Lawrence O. Gostin, \textit{Health Information Privacy}, 80 CORNELL L. REV. 451, 500 (1995) (stating each "agency that maintains a system of records must also, upon request, permit the individual to review and copy the record).

\textsuperscript{39} Roach, \textit{supra} note 14, at 98.

\textsuperscript{40} See Gilbreath v. Guadalupe Hosp. Found., 5 F.3d 785, 791 (5th Cir. 1993) (stating that hospitals "are not covered by the Act because they are not 'agencies' of the federal government within the meaning of the [Privacy Act]").


\textsuperscript{42} See Sean T. McLaughlin, \textit{Pandora's Box: Can HIPAA Still Protect Patient Privacy Under a National Health Care Information Network?}, 42 GONZ. L. REV. 29, 38 (2006). McLaughlin notes that "[r]egarding privacy safeguards, Congress sought to 'define and limit the circumstances in which an individual's protected health information may be used or disclosed by covered entities.'" \textit{Id.}

\textsuperscript{43} See Jurevic, \textit{supra} note 2, at 815. Jurevic states:

HIPAA requires health plans, health care clearinghouses, and health care providers that transmit health information in electronic form to maintain
create privacy rules under HIPAA, and when it failed to do so, the Department of Health and Human Services (HHS) assumed the power to create privacy rules. These privacy rules require health care providers to, among other things, limit their disclosure of confidential patient information and to notify patients when their confidential records have been disclosed. However, the text of HIPAA predicts that public safety is such a priority that there are many instances where the privacy rules established by the HHS will be superseded by the government’s desire to gain information about potential public health issues. There are three specific circumstances that the government can claim to override privacy rules for the public: national security circumstances, emergency circumstances, and general law enforcement circumstances. There are also a myriad of reasonable and appropriate administrative, technical, and physical safeguards that insure the integrity and confidentiality of the healthcare information. HIPAA also requires these individuals and groups to protect against any reasonably foreseeable threats or hazards to the security or integrity of the information. The individuals and groups must also protect against unauthorized uses or disclosures of the information and ensure compliance by their officers and employees.

44 See Swire & Steinfeld, supra note 11, at 1524. According to Swire & Steinfeld, “Congress initially contemplated that it would enact medical privacy legislation by the summer of 1999. When it did not do so, the Department of Health and Human Services assumed the power to issue a HIPAA privacy regulation.” Id.

45 See Swire & Steinfeld, supra note 11, at 1524-25. According to the authors, the federal regulation will now require health care providers, health plans, and health care clearinghouses to provide notice of their information practices; use and disclose protected health information only with patient permission, except in cases where designated national priorities warrant otherwise; permit patients to access and request correction of their records; provide patients an accounting of to whom their protected health information has been disclosed; limit the use and disclosure of protected health information to the minimum necessary amount; implement security safeguards to protect against unauthorized access or disclosure; and obtain satisfactory assurances, via a written contract, that their business associates using protected health information are protecting the privacy of that information.

46 See Swire & Steinfeld, supra note 11, at 1530 ("HIPAA specifically treats public safety as a national priority that, under certain circumstances, trumps the need to obtain patient permission for disclosures of health information.").

47 See Swire & Steinfeld, supra note 11, at 1530-32. The authors state that national security concerns can be stated to authorities without patient consent; that patients who present a risk to
other exceptions where personal medical information can be released without the consent of the subject of the information.48

With regard to states, the Model State Emergency Health Powers Act (MSEHPA) was created by the Center for Law and the Public's Health after the September 11, 2001, terrorist attacks against New York City and Washington, D.C. to provide a model law for states to use in balancing the privacy interests of patients with the desire of governments to access patient information in the event of a public health emergency.49 The MSEHPA was a response to the criticism that state laws relating to public health emergencies were antiquated, unable to respond, and too different to effectively combat an emergency.50 The MSEHPA purports to give states the right to respond appropriately to public health threats.51 Under the MSEHPA, states are permitted to collect records related to the medical information of the public, and investigators are allowed access to medical information on specific individuals in certain circumstances.52 The MSEHPA also requires health care providers to report any patient public safety, regardless of whether or not it is medically related, can be reported to authorities without consent, and; that law enforcement can request information from health care providers.  

Id.  

48 See generally 45 C.F.R. § 164.512. Among the reasons that personal medical information can be released without the individual's consent is for "public health activities", "if a person may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation..." 45 C.F.R. §164.512(b), (b)(iv). Other exceptions to the rule that personal medical information cannot be released without the consent of the individual are that information can be disclosed: "(1) to law enforcement officials; (2) to judicial and administrative proceedings; (3) for commercial marketing purposes; (4) to parents of unemancipated minors; (5) to "significant others," such as family members, close friends, or designated persons, of an adult or emancipated minor; (6) to an authorized public health authority; and (7) for health research." Gostin et al., supra note 18, at 16-17.  

49 See MSEHPA, supra note 16. According to The Center for Law and the Public Health, "The MSEHPA grants public health powers to state and local public health authorities to ensure a strong, effective, and timely planning, prevention, and response mechanisms to public health emergencies (including bioterrorism) while also respecting individual rights." Id. As of July 15, 2006, 38 states and the District of Columbia have enacted laws with provisions that are similar to, or taken from the MSEHPA. Id.  

50 See Matthew E. Brown, Reconsidering the Model State Emergency Health Powers Act: Toward State Regionalization in Bioterrorism Response, 14 ANN. HEALTH L. 95, 98 (2005) (stating that public health laws did not reflect advances in science and technology, particularly with respect to disease prevention).  

51 See MSEHPA, supra note 16 ("Emergency health threats, including those caused by bioterrorism and epidemics, require the exercise of essential government functions.").  

52 See MSEHPA, supra note 16. "[The MSEHPA] facilitates the early detection of a health
with the symptoms of any condition that could possibly be a cause of a public health emergency within 24 hours of the patient visiting the health care provider. The theory to which the MSEHPA ascribes is that the governments should have reserve power that may be used in emergency situations, but that this reserve power should be used in a way that minimizes the scope of the invasion of privacy to what is necessary to cope with the emergency.

President Bush, in an executive order on April 25, 2007, established the office of National Health Information Technology Coordinator (HITC) under the HHS. President Bush's goal in establishing the HITC was to use the newly established office to develop and maintain a national system of electronic health information that would allow information to flow easily between public and private offices. In directing DHHS to establish a national system for developing electronic health information, the government stated its purpose was to improve quality, accuracy and value in the delivery of health care. These objectives were reiterated in President Bush's 2006 State of the Union address, where his goals on the use of electronic health records were discussed in the context of a greater plan to control the costs of medical care. However, while the President has expressed a desire for a national standard for electronic medical records, Congress has not yet acted.
In addition to establishing the HITC, the DHHS and the Office of Management and Budget have created the Federal Health Architecture (FHA), an information technology office that seeks to monitor public health. The FHA seeks to develop an infrastructure for public health surveillance systems that will allow the federal system to interoperate with systems in the private sector and on the state level. The stated goals of the FHA do not include any specific goals related to privacy of confidential patient medical information. With respect to electronic medical records, the FHA has been developing a national standard for electronic information to be supplied to emergency health care providers, ostensibly to provide more effective care to patients.

While the FHA is the federal government’s attempt to use medical records for public health on a national level, local authorities are building large databases for health information. In 2006, New York City authorities created a database for storing the medical information of all diabetics in the city. The stated purpose of this new

---

60 See Mike Klein, Federal Health Architecture: An Interview with Kathleen Heuer, HHS, WISCONSIN TECHNOLOGY NETWORK, June 14, 2004, http://wistechnology.com/article.php?id=926 (last visited Nov. 4, 2008). While designed for public health surveillance, the FHA also encourages information sharing related to food safety, drug clinical trials, and medical research and development. Id.

61 See Department of Health and Human Services, Federal Health Architecture: Vision, Goals, Objectives and Milestones, available at http://www.hhs.gov/fedhealtharch/visions.html (last visited Nov. 4, 2008). According to the DHHS, “[I]t is best to demonstrate the benefit of the Federal Health Architecture by developing a target architecture for public health surveillance systems that can then be used to facilitate interoperability between surveillance systems across multiple agencies and in the national health community.” Id.

62 See id.

63 See Department of Health and Human Services, Federal Health Architecture: At-a-Glance, available at http://www.hhs.gov/fedhealtharch/AtaGlance.pdf (last visited Nov. 4, 2008) (“The Federal Health Architecture (FHA) Program supports federal health IT needs by providing a collaborative forum for creating a federal framework that is interoperable within the federal government, as well as between other public and private sector organizations”).

64 See infra notes 65-71 and accompanying text.

65 Harold J. Krent et al., Whose Business is Your Pancreas? Potential Privacy Problems in New York City’s Mandatory Diabetes Registry, 17 ANN. HEALTH L. 1, 1 (2008). The authors note that “[o]n January 15, 2006, New York City implemented a regulation requiring all testing labs in the city to report the test results of all A1C diabetes test subjects to the New York City Department of Health and Mental Hygiene.” Id. at 2. The regulation required all laboratories in New York City send the following information to the Department of Health and Mental Hygiene: the full name, date of birth, and address of the diabetic; the medical record number if known; the identification number or code assigned to the diabetic; the name and address of the physician or clinical laboratory who
database was to utilize the data to confront the rise in diabetes cases in New York City. Among residents of New York City, diabetes is the fourth largest cause of death. This is the first American government database of its kind that does not seek to track those who are diagnosed with a communicable disease. However, Sweden and Belgium have already created databases to track persons who have diabetes. These databases only allow for further contact with a patient listed in the database with the affirmative consent of the patient. Under the New York City database, personal information from the database about a particular patient could be released to a researcher without violating any provision of the regulation that formed the database.

International Standards for Medical Record Privacy

The European Union (EU) passed a Directive on the Protection of Personal Data in 1995 (EU Directive) that included protections on health information in protecting all personal data. Like the MSEHPA, the EU Directive allows for exceptions related to disclosure of medical information when circumstances require it. There are exceptions that allow health care providers to use patient data in a way consistent with medical aims, but these exceptions have requirements that specific safeguards are put in place to protect the privacy of the patients whose data is being used. The EU Directive required that all EU member states put in place safeguards for privacy at the very least as stringent as the EU Directive itself. The United Kingdom submitted the blood specimen; the name and address of the clinical laboratory which performed the test; the date the test results were first available; and the name(s) of any other tests performed in addition to the diabetes test. Id. at 3-4.

66 Id. at 2.
67 Id. at 4. The number of diabetic residents of New York City has doubled in the past ten years. See id.
68 Id. at 10. Other databases have been created, including the Vermont Diabetes Information System (VDIS) sponsored by the National Institute of Health. Id. The difference between the VDIS and the New York City database is that the VDIS is voluntary and patients can opt out of it. Id.
69 See Krent et al., supra note 65, at 11.
70 Id.
71 Id. at 18-19.
72 See Jurevic, supra note 2, at 813.
74 See id.
75 See Jurevic, supra note 2, at 813. As Jurevic notes, “[t]he Directive is a framework that establishes principles with which the fifteen Member States must bring their national laws, regulations, and administrative provisions into conformance with the Directive by October
passed its Data Protection Act in 1998. Information related to one's health is listed as "sensitive personal data" under the Data Protection Act.

Private Industry Movements into Medical Record Use

Private companies with primary businesses outside of the medical industry are increasingly interested in the storage of electronic medical records. Google recently announced plans to work with the Cleveland Clinic to allow volunteers to access their medical records on an internet website run by Google before the end of 2008. In October 2007, Microsoft, in partnership with the American Heart Association, Johnson & Johnson LifeScan, New York-Presbyterian Hospital, and the Mayo Clinic, among others, founded HealthVault, a system for storing personal medical records on a database. HealthVault allows patients to store their electronic medical records on a Microsoft server and features tailored search options available based on those medical records. While Microsoft and Google may be the most well-known companies entering the electronic medical records storage industry, other companies, such as Revolution Health and WebMD, are entering the field of electronic medical record storage.

III. Problems With Giving the Government Unlimited Access to Medical Records

Electronic Medical Records are Very Susceptible to Misuse

There is always a risk that the government will seek information for purposes that bear a dubious connection to the purpose of protecting public health. Giving the

1998.” Id.
76 See Data Protection Act of 1998, 1998, c. 29 (Eng.).
77 See Data Protection Act of 1998, 1998, c. 29, § 2 (Eng.).
78 See Richard Waters, Google Reveals Plans for Health Database, FIN. TIMES, February, 29, 2008, at 20 (describing Google's efforts to create a digital health records database).
79 See Victoria Colliver, Medical Info Online is Closer; Google Prepars to Let Patients Handle Records Digitally, SAN FRAN. CHRON., Feb. 29, 2008, at C1.
83 See generally Tucson Woman's Clinic v. Eden, 379 F.3d 531 (9th Cir. 2004). Arizona enacted a statute in 1999 that allows its Department of Human Services to review medical information
government the ability to collect records in electronic form only heightens the risk that the government will violate patients' privacy.\textsuperscript{84} Electronic medical records are very transferable, whereas with a paper medical file, the patient could be assured by the knowledge that while hard copies could be made of their records, logistically, hard copies are more difficult to disseminate.\textsuperscript{85} To offset the heightened risk that electronic medical records will be misused, much stronger protections need to be in place in order to prevent the government from violating patient privacy.\textsuperscript{86} It is possible that invocation from patients of doctors performing more than five abortions without any provision that protects patient information from public release. \textit{Id. See also} Mariner, \textit{supra} note 6, at 384 (stating that there is no clear idea of what “public health” is).

\textsuperscript{84} See \textit{generally} Gostin, \textit{supra} note 7 (arguing that public health agencies seek “power without constraint”).

\textsuperscript{85} See \textit{generally} Boyer, \textit{supra} note 12, at 38-39. Electronic medical records can be transferred to other computers, copied, and stored for an indefinite period of time. \textit{Id.}

\textsuperscript{86} See Mariner, \textit{supra} note 6, at 382-383 (listing desired requirements for reporting patient information in the absence of an “investigatory need”). The author’s desired considerations are:

(1) whether the information is personally identifiable (contains personal information sufficient to identify the individual whose information it is);

(2) whether the information is collected with or without the person’s consent;

(3) what present or future uses will be made of the information;

(4) whether subsequent uses will be with or without the person’s consent;

(5) whether the information will be combined or linked with information from other sources to create new information;

(6) whether the combined or linked information makes it possible to identify individuals;

(7) whether the information will be disclosed by the recipient to third parties;

(8) whether the information will be re-disclosed by the third parties to fourth and fifth parties;

(9) whether the information will be kept secure and inaccessible to anyone without authorization to view it;

(10) whether the information will be kept or destroyed after use by each user;

(11) whether the information will be kept confidential by those authorized to view it; and

(12) whether there is an enforceable (statutory or contractual) duty to keep the information secure and confidential on the part of all parties (recipient, third parties, etc.).
of hot-button issues, such as the threat of bioterrorism, even where no credible threat exists, could tip the balancing test used in Whelan and Westinghouse Electric Corp. in favor of disclosure to the government.\footnote{See United States v. Westinghouse Electric Corp., 483 F. Supp. 1265, 1271 (W.D.PA 1980); Whelan v. Roe, 429 U.S. 589 (1977). See also Mariner, supra note 6, at 394. “In a post-September 11 world, where epidemics are both rare and terrifying, emergency preparedness has encouraged more expansive public health surveillance programs with links to multiple independent sources of information.” Id.}

**Privacy Concerns are Ignored In Times of “Emergency”**

The MSEHPA has no provisions for the privacy of medical records.\footnote{See Ken Wing, Policy Choices and Model Acts: Preparing for the Next Public Health Emergency, 13 HEALTH MATRIX 71, 75 (2003). Wing states that “there are no provisions for the protection of confidentiality or privacy written into the [MSEHPA], although, in a later article of the [MSEHPA] the authors have had the foresight to immunize public officials from liability for exceeding their powers.” Id.} Courts are not always on the same page as the government in identifying what an emergency is, which has the potential of creating situations where the government gets more access to patient records than necessary, but also allows the risk that the government may not be able to get access to medical records in those infrequent instances where they will be necessary for public health.\footnote{See Mariner, supra note 6, at 384 (stating that courts have an unclear view as to what “public health” means).} The MSEHPA gives a vague definition of what a public health emergency is, and this definition could be manipulated to meet the perceived needs of government.\footnote{See MSEHPA, supra note 16, at 11. Under the MSEHPA, a “public health emergency” is: an occurrence or imminent threat of an illness or health condition that: (1) is believed to be caused by any of the following: (i) bioterrorism; (ii) the appearance of a novel or previously controlled or eradicated infectious agent or biological toxin; (iii) [a natural disaster]; (iv) [a chemical attack or accidental release; or] (v) [a nuclear attack or accident]; and (2) poses a high probability of any of the following harms: (i) a large number of deaths in the affected population; (ii) a large number or serious or long-term disabilities in the affected population; or (iii) widespread exposure to an infectious or toxic agent that poses a significant risk of substantial future harm to a large number of people in the affected population. Id. at 11. The MSEHPA does not define many of the terms in the proposed definition of “public health emergency,” such as “natural disaster” or “large number.” Id.} Hastily created in the aftermath of the attacks of September 11, 2001, and the anthrax mailings in the month after those attacks, the MSEHPA tends to
allow the government access to information first, worrying about privacy of patients later. Situations warranting government access to medical records, for example, where there is a “public health emergency” or “national disaster,” should be defined in a manner that prevents government abuse. When given a choice between interpreting a statute in a way that limits or expands power, government agencies tend to interpret statutes to expand their power. Defining circumstances that justify government access to medical records will prevent the usage of vague statutes to expand power in this way. The MSEHPA provision allowing the government to gain access to medical records when an executive branch declares a “public health emergency” should be limited to short periods of time. To deal with the possibility of a long-term public health emergency, the statute should be limited to a short period of time.

---

91 See Erickson et al., supra note 54, at 60. “Planning and surveillance [of patients] would be implemented immediately, but the measures affecting property and persons would be triggered only after a state’s governor declares a public health emergency.” Id.
92 See MSEHPA, supra note 16, at 12. The MSEHPA definition of “public health emergency” uses phrases such as “natural disaster” and “a large number of deaths” that are vague and contain the ability to be manipulated. See id. See also Mariner, supra note 6, at 384-385. According to Mariner:

[a] more rigorous approach to balancing government and individual interests might be accomplished by abandoning vague characterizations of the government's interest, like public health, and substituting the government's actual intended use of information at each level of surveillance. The distortions currently permitted by vague terminology on both sides of the balancing test might be mitigated by more precise definitions of the interests to be weighed and by assigning realistic present values to those interests, in a manner analogous to decision analysis.

Id.
93 See Gostin, supra note 7, at 1162. As Gostin notes:

[p]ublic health policy is riddled with contradictions. Agency officials seek power without constraint. Since they are ‘experts,’ they resist substantive or procedural fetters on their decisions. Public health officials often distrust the lay public or their elected representatives, believing they do not understand the sciences of public health and are ill-suited to make sound judgments about infectious disease.

Id. See also Mariner, supra note 6, at 385. “The distortions currently permitted by vague terminology on both sides of the balancing test might be mitigated by more precise definitions of the interests to be weighed and by assigning realistic present values to those interests, in a manner analogous to decision analysis.” Id.
94 See Mariner, supra note 6, at 385 (arguing that the government’s interest needs to be defined to prevent misuse of medical records).
health emergency and to ensure that one branch of government does not violate personal privacy for a needlessly extensive period of time, there should be a provision allowing the grant of access to be extended where a supermajority of the Congress or state legislature in the jurisdiction where the government declared the "public health emergency" gives its approval.96

The United States needs to ensure that privacy when storing and collecting medical information from patients is paramount by allowing medical providers to determine the software used for electronic health record maintenance.97 Medical providers already have various software platforms to choose from in storing electronic medical records.98 Whichever method a health provider uses, giving patients the option to opt out of electronic maintenance of their medical records is extremely important; if electronic medical records give the government an easier way to violate personal privacy, the individual must have an effective way to counteract this.99 Personal privacy is not

96 See Marks, supra note 95, at 598-99 (discussing similar proposal derived at Yale Law School where President could declare state of emergency, with extensions granted only by gradually increasing supermajorities of Congress).
97 See Terry & Francis, supra note 3, at 686. The George W. Bush administration favors letting the health care industry develop its own standards for privacy. See id. As the authors note "[t]he Bush administration publicly eschews any regulatory mandate directing healthcare providers to adopt [electronic health records]. Rather, it espouses EHR adoption via "a smooth market-led way." Id.
98 See Terry & Francis, supra note 3, at 685-88. Providers can choose between software programs, including: Electronic Health Records systems that allow for sharing electronically between medical providers and the government at a local, state and national level; Continuity of Care Record, that allow health providers to use proprietary systems for maintaining medical records and transferring records between providers through paper and/or computer files, and; Personal Health Records, electronic records that are maintained and stored by the patient and cannot be transferred between health providers. Id.
99 See Terry & Francis, supra note 3, at 696. Patients cite privacy as an issue of great concern with electronic medical records.

Patients cite privacy, together with security, as their issues of greatest concern about electronic records. The International Medical Informatics Association lists patient privacy (and confidentiality) as a core ethical principle: "All persons have a fundamental right to privacy, and hence to control over the collection, storage, access, use, communication, manipulation and disposition of data about themselves." Data from several recent surveys indicate that privacy protection remains highly salient for patients and that this salience may be even greater among patients with diagnoses of illness and among racial and ethnic minorities. According to a 2005 survey conducted by the California HealthCare Foundation, 67% of Americans are concerned about the privacy of
just an issue for the safety of medical records; for a substantial number of people, privacy concerns actually keep them from seeing a doctor.\textsuperscript{100} If a patient's fear for her personal privacy will stop her from seeing a doctor, the benefit the government seeks in obtaining information from electronic medical record and an accurate statement of the patient's symptoms and diagnoses will be lost.\textsuperscript{101}

In creating the HIPAA Privacy Rule, HHS noted a correlation between a patient's lack of faith in the privacy of their medical information and the quality of care the patient receives.\textsuperscript{102} The MSEHPA provision that creates criminal penalties to ensure their health records. An even greater percentage (73\%) of ethnic and racial minority patients in the survey expressed concern about the privacy of health information.

\textit{Id.}  
\textsuperscript{100} See Terry & Francis, \textit{supra} note 3, at 697. A 2005 study done by the California HealthCare Foundation found that one in eight respondents performed an action that may "have compromised their health care," such as avoiding a doctor or avoiding medical tests, in the interest of protecting their privacy. \textit{Id.} See Roger E. Harris, \textit{The Need to Know Versus the Right to Know: Privacy of Patient Medical Data in an Information-Based Society}, 30 SUFFOLK U. L. REV. 1183, 1197-1198 (1997). According to Harris, "[t]he effects of improper access and disclosure not only impact the individuals whose medical information is compromised, but also negatively affect a medical provider's ability to furnish quality care because privacy violations engender a 'chilling effect' that prevents patients from communicating fully about their medical problems with their physician." \textit{Id.} See also Peter A. Winn, \textit{Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law}, 33 RUTGERS L. J. 617, 622 (2002). According to Winn:

The dangers associated with disclosure of personal health information have a strong practical impact on the relationship of trust between a patient and a physician. The doctor must trust the patient to give full and truthful information about her health, symptoms, and medical history. The patient must trust the doctor to use that information on behalf of the patient and to keep the information confidential. If a patient believes that a doctor will not keep his or her medical information confidential, the patient may not be willing to tell the truth about sensitive personal matters. If a doctor is not provided truthful information, the doctor will be unable to render proper care to the patient, and the doctor's ability to treat the patient may be impaired.

\textit{Id.}  
\textsuperscript{101} See Harris, \textit{supra} note 100, at 1198. Privacy fears cause patients to be untruthful with doctors and "neutralizes the health benefits associated with medical information contained in the primary information sector and available to those providing direct patient care." \textit{Id.}  
compliance suggests that the government may regard citizens as adversaries when compiling medical records.\textsuperscript{103} This will keep patients from feeling that their privacy is secure.\textsuperscript{104} The government also sees the ability to compile medical records of the public as a net positive, and thus focus its efforts on keeping the information out of public view, as opposed to considering the limitation of how much the government may have access to in the first place.\textsuperscript{105}

The public should not allow the government to access their medical records simply on the basis of an unsubstantiated bioterror threat.\textsuperscript{106} As the health care industry moves further with electronic records, these records will become invaluable to the government in the event of an actual emergency, provided that privacy safeguards are in place to allow patients to feel secure to visit their health care providers and be honest with them while they are there.\textsuperscript{107} But while electronic medical records will allow the

\begin{quote}
[Individuals cannot be expected to share the most intimate details of their lives unless they have confidence that such information will not be used or shared inappropriately. Privacy violations reduce consumers' trust in the health care system and institutions that serve them. Such a loss of faith can impede the quality of the health care they receive, and can harm the financial health of health care institutions.]
\end{quote}

\textit{Id.}

\textsuperscript{103} See, Marks, supra note 95, at 594. According to Marks,

\begin{quote}
The [MSEHPA] was premised on a model of non-cooperation by both medical personnel and citizens in the event of a bioterrorist attack. In addition to powers of isolation and quarantine, the [MSEHPA] relied on criminal law to coerce compliance: any person refusing to be examined, tested, or vaccinated would be liable for a misdemeanor, as would any health care provider who refused to perform an examination or test.
\end{quote}

\textit{Id.}

\textsuperscript{104} See Marks, supra note 95, at 594 (stating that the MSEHPA Act "was premised on a model of non-cooperation by both medical personnel and citizens in the event of a bioterrorist attack").


\textsuperscript{106} See generally George J. Annas, \textit{Puppy Love: Bioterrorism, Civil Rights and Public Health}, 55 FLA. L. REV. 1171 (2003) (asserting that bioterrorism threat is no more of a threat to the United States than "nuclear or conventional bombs;" and that an assertion otherwise is the false premise behind proposed emergency public health legislation). Annas argues that "[p]ublic health planning should be based on science, especially the science of epidemiology and accurate risk assessment and facts, not the free-floating anxiety and fear that the government uses to justify more control over individual citizens." \textit{Id.} at 1178.

\textsuperscript{107} See Gostin, supra note 7, at 1133-34. Gostin states that "[s]urveillance, like intelligence in the
government comprehensive, exhaustive information about patients who show symptoms that could concern public health, governmental use of these medical records could also mean the restriction of patients’ civil liberties in a way that adds nothing to the protection of public health. Using exhaustive medical records to identify individual patients who presented symptoms similar to those that occur in a bioterror attack could allow the government the ability to cast an arbitrarily defined “safety net” to locate and force all people with these symptoms into healthcare providers for supplementary tests without forcing the government to give any cause.

Currently, there are terabytes of electronic medical records on scattered servers and databases in health care facilities around the country. While many of these records are on servers that are disconnected, as companies like Microsoft and Google enter the business of storing electronic medical records online, it is only a matter of time before these terabytes of medical records are placed on servers that interconnect. Also, considering that some proponents of giving the government more access to medical records see increased public health surveillance as one of the primary ways to stop a potential bioterror attack, the prospect of having electronic medical record databases on a national scale operated by Google may become too irresistible for the government to pass up.

See Annas, supra note 106, at 1181-82. According to Annas “[u]nfortunately, bad state public health emergency laws are not only dangerous to liberty, they are a danger to public health itself. They can make it much more likely that a bioterrorist attack will be poorly managed by encouraging public health officials to act in counterproductive ways that undermine public trust and actually promote fear and panic.” Id.

See Annas, supra note 106, at 1186. Annas states that a model public health act in Florida allows a government health officer to identify patients as “qualified” because of certain symptoms and force the “qualified” to be “examined, tested, vaccinated, treated or quarantined.” Id.

See Greene, supra note 81. A terabyte is 1,000,000,000,000 (one trillion) bytes of data. Techweb.com, Techencyclopedia, http://www.techweb.com/encyclopedia/defineterm.jhtml?term=terabyte&x=&y= (last visited Nov. 4, 2008).

See Colliver, supra note 79; see also Lohr, supra note 80.

See Gostin, supra note 7, at 1128-29 (stating that the threat of bioterror is compounded by the inability of public health agencies to detect it effectively).
IV. Conclusion

As long as medical records technology moves toward a comprehensive system of electronic medical recordkeeping, the balancing test in Westinghouse Electronic Corp. between the patient and the government will go the government's way, without more concrete protections of who can access the records and for what reason. The government will continue to encourage the health care industry to computerize their records, ostensibly for reasons that mention more accurate care and saving money, but without being honest about the government's desire for access to the newly created databases. Companies like Google and Microsoft will move into electronic medical records storage, allowing the patient better access to their health information, but these companies may fail to take the steps necessary to keep access away from the government.

Electronic medical records are susceptible to misuse, and the proposed MSEHPA will give states the ability to obtain electronic medical information on citizens on a potentially dubious claim of a "public health emergency." Because of this, privacy provisions for electronic medical record use need to be strengthened before the next public health emergency so that the balancing test previously used is replaced with specific rules tailored guided by the principle that the medical record data is not allowed to be used by the government. Allowing medical records database owners, such as health care providers, the ability to generally apprise the government of certain trends without supplying personally identifiable information will protect public health the same. However, as private companies build larger and more interconnected databases, the government's interest in getting access to these databases will only grow.