ELECTRONIC HEALTH RECORDS: HOW THE UNITED STATES CAN LEARN FROM THE FRENCH DOSSIER MÉDICAL PERSONNEL

AMANDA GRADY*

ABSTRACT

Although the adoption of a Nationwide Health Information Network (NHIN) was made a priority in recent health reform legislation, the United States trails many countries, including France, in its development of a national health information exchange (HIE). Even though France faced considerable challenges in its efforts to implement a similar system, the *Dossier Médical Personnel* (DMP) was authorized for use by clinicians in 2011. Implementation of the DMP offers a unique opportunity for the United States to learn from the challenges France has faced as it attempts to achieve widespread use of electronic health records (EHRs) by 2014.

The United States can learn from the challenges France faced in implementing a national, interoperable health information exchange that also safeguards patient privacy. While development of such a system is still in its early stages in the United States, the overemphasis of either interoperability or patient privacy at the expense of another slowed progress in both countries. In France, patient privacy was prioritized, while in the United States, the primary focus has been on NHIN

* J.D., University of Wisconsin Law School, 2012; M.P.H., Emory University, 2007; B.A., University of Chicago, 2005. I would like to thank the editors and staff of the Wisconsin International Law Journal for their assistance throughout the writing and editing process. I would also like to thank University of Wisconsin Law School Professor Kathleen Noonan for reviewing an early draft of this article and providing invaluable feedback and support. Finally, I would like to thank my friends and family for their love and support.

infrastructure and technology standards. This paper argues that a successful health information exchange system cannot exist unless policies related to patient privacy are balanced with investments in infrastructure and delivery systems.

INTRODUCTION

The phrase "Electronic Health Record" (EHR) is commonly defined as a longitudinal health record with entries by healthcare practitioners in multiple sites where care is provided.[1] The EHR contains all information traditionally found in a patient's health record, including demographic information, progress notes, medications, past medical history, immunization history, laboratory results, and radiology reports.[2] However, unlike paper records, it allows information from multiple providers to be included.[3] Thus, an EHR should contain the entire health history of a patient throughout his or her life, facilitating a more efficient

---

1 WORLD HEALTH ORG. [WHO], ELECTRONIC HEALTH RECORDS: MANUAL FOR DEVELOPING COUNTRIES 12 (2006) [hereinafter WHO].

2 *EHR: Electronic Health Record*, HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS, http://www.himss.org/ASP/topics_ehr.asp (last visited May. 1, 2012).

3 WHO, *supra* note 1, at 12.

way for health care providers to share and access health information than the traditional paper record.[4]

According to the Centers for Medicare and Medicaid Services, a "medical record is considered complete if it contains sufficient information to identify the patient; support the diagnosis/condition; justify the care, treatment, and services; document the course and results of care, treatment, and services; and promote continuity of care among health care providers."[5] An electronic medical record (EMR) is a computerized medical record used by healthcare providers to "document, monitor, and manage health care delivery within a care delivery organization."[6] The EMR contains the same data found in a paper medical record and may also include decision support algorithms, such as a program to alert a physician about potential drug interactions.[7] However, an EMR only contains information from one care delivery organization.[8] An EHR, on the other hand, is a summary of the information contained in an individual's EMRs from multiple care delivery organizations throughout the life of the individual.[9] In the United States, the proposed NHIN will allow EHRs to be accessed throughout the country, forming a health information exchange (HIE).[10]

Proponents of EHRs believe that this increased efficiency will improve coordination of care between private physicians, hospitals, labs, and other organizations and institutions that provide health care services.[11] Many studies have proven that EHR databases are a cost-effective way to reduce medical errors due to disorganized and

---

4 *See id.*

5 *Revised Appendix A, "Interpretive Guidelines for Hospitals,"* CENTERS FOR MEDICARE & MEDICAID SERVICES (June 5, 2009), https://www.cms.gov/transmittals/downloads/R47SOMA.pdf.

6 Dave Garets & Mike Davis, *Electronic Medical Records vs. Electronic Health Records: Yes, There Is a Difference* 2 (2006), http://www.himssanalytics.org/docs/WP_EMR_EHR.pdf.

7 *Id.*

8 *Id.*

9 *Id.* at 2–3. Although some sources use the terms EMR and EHR interchangeably, this paper will use the definitions proposed by the Healthcare Information and Management Systems Society (HIMSS). *Id.* at 2.

10 *See, e.g., id.* at 2–3 ; *see also* AHIMA e-HIM Work Group on the Legal Health Record, *Update: Guidelines for Defining the Legal Health Record for Disclosure Purposes*, 76 J. AHIMA 64A (2005) (discussing types of applications and health-related information that may be included in an EHR).

11 *See* Richard Hillestad et al., *Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs*, 24 HEALTH AFFAIRS 1103, 1103 (2005).

inaccessible patient data, thus improving medical care.[12] EHRs can be programmed to use algorithms that take current and past clinical information into account in order to provide treatment recommendations during a clinical encounter.[13] For example, an EHR can be used to check for possible drug interactions between a patient's existing medications and a new prescription.[14] Furthermore, EHR advocates argue that costs associated with duplicative care will be reduced.[15] For example, if a patient seeks a second opinion after one physician's diagnosis, the second physician can easily determine which tests have already been performed and obtain the results of those tests. Finally, a national database of population health measures will improve public health reporting.[16]

In the United States, the Institute of Medicine has long recommended the use of health information technology and has urged "a renewed national commitment to building an information infrastructure to support health care delivery, consumer health, quality measurement and improvement, public accountability, clinical and health services research, and clinical education."[17] The nationwide adoption of EHRs in order to facilitate the development of the NHIN is an important part of recent healthcare reform legislation signed into law by President Obama.[18] In support of this legislation, the President said, "We will make the immediate investments necessary to ensure that within five years all of America's medical records are computerized."[19] President Obama has also stated that "[d]igital medical records could prevent medical errors,

---

[12] James G. Anderson, *Social, Ethical, and Legal Barriers to E-Health*, 76 INT'L J. MED. INFORMATICS. 480, 480 (2007).

[13] WHO, *supra* note 1, at 12.

[14] Ryan P. Radecki and Dean F. Sittig, *Application of Electronic Health Records to the Joint Commission's 2011 National Patient Safety Goals*, 306 JAMA 92, 93 (2011).

[15] *Benefits of EHRS: Medical Practice Efficiencies and Cost Savings*, HEALTHIT.GOV: ADVANCING AMERICA'S HEALTHCARE, http://www.healthit.gov/providers-professionals/medical-practice-efficiencies-cost-savings (last visited May 24, 2012).

[16] *See generally id.*; Anna O. Orlova, et al., *An Electronic Health Record—Public Health (EHR-PH) System Prototype for Interoperability in 21st Century Healthcare Systems*, 2005 AMIA ANNUAL. SYMPOSIUM PROCEEDINGS 575, 575–76 (2005).

[17] INST. OF MED., CROSSING THE QUALITY CHASM: A NEW HEALTH SYSTEM FOR THE 21ST CENTURY 166 (2001) [hereinafter IOM].

[18] *Health Reform Law Builds on Electronic Health Record Incentive Program*, BARNES & THORNBURG (Apr. 8, 2010), http://www.btlaw.com/files/ALERT%20-%20Healtchare_Electronic%20Health%20Record%20Incentive%20Program.pdf.

[19] Robert Pear, *Privacy Issue Complicates Push to Link Medical Data*, N.Y. TIMES, Jan. 18, 2009, at A16, *available at* http://www.nytimes.com/2009/01/18/us/politics/18health.html.

save lives and create hundreds of thousands of jobs."[20] In addition to strengthening federal medical privacy law, one of the goals of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of the 2009 American Recovery and Reinvestment Act (ARRA), is to encourage a greater number of physicians and physician organizations to adopt EHRs as a first step toward a NHIN.[21] The ARRA allocated $19 billion to develop health information technology infrastructure and to encourage doctors, hospitals, and other providers through Medicare and Medicaid incentives to achieve "meaningful use"[22] of electronic health records by 2015.[23]

Similarly, the push for the development of a national HIE in France began as part of a healthcare reform movement in the early 2000s.[24] As in the United States, the goals of this movement were to control medical costs and improve quality of care.[25] Then-Minister of Health Philippe Douste-Blazy said, "Firstly, the government intends to promote an effective coordination of health care. The most efficient tool for such coordination is the personal medical record."[26] The *Dossier Médical Personnel* (DMP) was introduced as part of the Health Insurance Reform Act in August 2004.[27] Although the French government initially wanted the DMP to be ready for use in 2007, the

---

[20] *Id.*

[21] Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 115-5, §13101, Sub. A, § 3001, 123 Stat. 115, 92–101 (2009). "This bill promotes the use of health information technology (health IT), such as electronic health records, by: requiring the government to take a leadership role to develop standards by 2010 that allow for the nationwide electronic exchange and use of health information to improve quality and coordination of care; investing $19 billion in health information technology infrastructure and Medicare and Medicaid incentives to encourage doctors, hospitals, and other providers to use health IT to electronically exchange patients' health information; and strengthening Federal privacy and security law to protect identifiable health information from misuse as the health care sector increases use of health IT." SENATE FINANCE, HOUSE WAYS & MEANS COMMITTEES, THE AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009—FEBRUARY 12, 2009 18 (2009) [hereinafter ARRA SUMMARY].

[22] *See infra* note 159.

[23] ARRA SUMMARY, *supra* note 21, at 18; BARNES & THORNBURG, *supra* note 22.

[24] LAURENCE ESTERLE, NATIONAL REPORT OF EHR IMPLEMENTATION 14 (2009) [hereinafter EHR-Implement].

[25] Victor G. Rodwin & Claude Le Pen, *Health Care Reform in France: The Birth of State-Led Managed Care,* 351 NEW ENG. J. MED. 2259, 2260 (2004).

[26] *See* EHR-Implement, *supra* note 24, at 18.

[27] *Id.*; J. ARTMANN & S. GIEST, EUROPEAN COMMISSION, COUNTRY BRIEF: FRANCE 16–17 (2010), http://ehealth-strategies.eu/database/documents/France_CountryBrief_eHStrategies.pdf.

project ran into a number of difficulties and was halted in 2008.[28] The DMP was later reintroduced and, and the new version was launched in December 2010.[29]

While both countries have embraced the concept of national EHR databases as a way to improve coordination of care and reduce medical costs, the implementation of this technology has not been widely successful in the United States. There is much debate about whether a national HIE exchange that also safeguards patient privacy is possible.[30] In addition to the need to address data privacy and security concerns, full EHR interoperability requires uniform national technology standards in order to ensure that health care providers are able to share records contained in EHR databases from different vendors.[31] Although France has successfully implemented a national HIE exchange, the United States continues to face difficulties. Therefore, an analysis of France's efforts could illuminate ways for the United States to approach and resolve likely barriers.

This paper asserts that the United States can learn from the challenges France faced in developing a national, interoperable health information exchange that safeguards patient privacy. In particular, successful implementation of a national HIE will require comprehensive, national laws that protect patient privacy and provide for the interoperability of these databases. The first part discusses and compares the development of EHR databases in the United States and France. The second part considers the barriers to implementation that each country has faced. The third part analyzes strategies that the United States could use to overcome these barriers based on the experience that France has had. This paper concludes by stressing the importance of addressing patient privacy concerns and standardizing the privacy laws and other regulations governing EHRs and the system itself before beginning implementation.

---

[28] ASIP SANTÉ, *The DMP: A Project that is Structuring the Development of e-Health in France* (June 21, 2010), http://esante.gouv.fr/en/actus/dmp/dmp-a-project-structuring-development-e-health-france.

[29] ASIP SANTÉ, RAPPORT D'ACTIVITÉ 2010–11 (2010), http://esante.gouv.fr/sites/default/files/ASIP_RA2010.pdf.

[30] John R. Christiansen, *Legal Speed Bumps on the Road to Health Information Exchange*, 1 J. HEALTH & LIFE SCI. L. 1, 1 (2008).

[31] *See* HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, INTEROPERABILITY DEFINITION AND BACKGROUND (June 9, 2005), http://www.himss.org/content/files/interoperability_definition_background_060905.pdf.

I. HISTORY OF EHR DEVELOPMENT

The first known medical record was developed by Hippocrates in the fifth century, B.C.[32] He believed that a medical record should accurately reflect the course of a disease as well as indicate the likely cause of disease.[33] This concept remains important today, as providers in the United States and France have recognized the need for accurate and efficient flow of patient medical information between providers in order to improve preventative treatment and the continuity, coordination, and quality of care.[34] EHR implementation in both countries is being driven by business concerns, including error and cost reduction.[35] In the United States, characteristics of managed care, such as the data needs of "gatekeeper" physicians, require an increased need for risk management tools, and demands for measurement of quality indicators.[36]

A. EHR DEVELOPMENT IN THE UNITED STATES

The U.S. healthcare system has been described as a "cottage industry" because it is fragmented at the national, state, community, and individual practice level.[37] Even though the Federal government is the largest payer of healthcare costs, there is no national body of law or policy that governs the system exclusively.[38] At the state level, multiple public and private agencies are responsible for monitoring and providing care, while at the community level, health care providers serving the same patient populations rarely communicate with one another.[39] Health care is paid for through a combination of public and private financing with multiple payers.[40] Nearly 56% of Americans with health insurance are covered by an employment-based health insurance plan.[41] Just over

---

[32] M.A. MUSEN, HANDBOOK OF MEDICAL INFORMATICS 99 (J.H. van Bemmel & M.A. Musen, eds., 1997).

[33] *Id.*

[34] *See* IOM, *supra* note 17; *see* ASIP SANTÉ, *supra* note 28.

[35] *See* IOM, *supra* note 17, at 3; *see* ASIP SANTÉ, *supra* note 28.

[36] IOM, *supra* note 17.

[37] ANTHONY SHIH, ET AL., COMMONWEALTH FUND, ORGANIZING THE U.S. HEALTH CARE DELIVERY SYSTEM FOR HIGH PERFORMANCE ix (2008).

[38] *Id.*

[39] *Id.*

[40] MICHAEL K. GUSMANO ET AL., HEALTH CARE IN WORLD CITIES: NEW YORK, PARIS, AND LONDON 26 (2010).

[41] CARMEN DENAVAS-WALT ET AL., U.S. CENSUS BUREAU, HEALTH INSURANCE COVERAGE IN THE UNITED STATES: 2009, at 25 (2010).

30% of Americans with health insurance are covered by government health insurance programs, including Medicare, Medicaid, and military health care.[42]

Given the fragmentation of the U.S. health care delivery system, a national EHR database appears to be a way to improve the "safety, quality, and efficiency of health care in the United States."[43] The first EMRs, which contained information about a patient's medical care within one health care delivery organization, were developed in the 1960s.[44] Within that decade, clinical information projects were underway at 73 hospitals, and 28 projects for medical document storage and retrieval were in progress.[45] Many of the EHRs in use today are based on these early EMRs developed in academic medical centers and government clinical care organizations, like the system used by the Veteran's Administration.[46]

Much of the recent push toward EHR implementation has come from the federal government. In 2001, the National Committee on Vital and Health Statistics (NCVHS) published a report that called for the federal government to direct the development of the National Health Information Infrastructure.[47] The Office of the Assistant Secretary for Planning and Evaluation started an initiative in 2002 to begin implementation of the NCVHS recommendations, which urged the creation of a new office within the Department of Health and Human Services to oversee and coordinate progress of this initiative.[48]

Among other measures, the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 called for the creation of a

---

[42] *Id.* The estimates by type of coverage are not mutually exclusive, as people can be covered by more than one type of health insurance. *Id.*

[43] IOM, *supra* note 17.

[44] *See* NATIONAL INSTITUTES OF HEALTH, NATIONAL CENTER FOR RESEARCH RESOURCES, ELECTRONIC HEALTH RECORDS OVERVIEW 2 (2006), *available at* http://www.ncrr.nih.gov/publications/informatics/ehr.pdf (" In 1965, Summerfield and Empey reported that at least seventy-three hospital and clinical information system projects and twenty-eight projects for storage and retrieval of medical documents and other clinically relevant information were under way.").

[45] *Id.*

[46] *Id.*

[47] U.S. GOV'T. ACCOUNTABILITY OFFICE, GAO-04 2 -991R, HHS'S EFFORTS TO PROMOTE HEALTH INFORMATION TECHNOLOGY AND LEGAL BARRIERS TO ITS ADOPTION 14–15 (2004).

[48] U.S. GOVT. ACCOUNTABILITY OFFICE, GAO-04-991R, HHS'S EFFORTS TO PROMOTE HEALTH INFORMATION TECHNOLOGY AND LEGAL BARRIERS TO ITS ADOPTION 14–15 (2004); NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS, INFORMATION FOR HEALTH: A STRATEGY FOR BUILDING THE NATIONAL HEALTH INFORMATION INFRASTRUCTURE 3 (2001), *available at* http://www.ncvhs.hhs.gov/nhiilayo.pdf.

Commission on Systemic Interoperability to develop a framework for the implementation of national health care information technology (IT) standards in response to these initiatives.[49] In 2004, President Bush passed an executive order establishing the Office of the National Coordinator for Health Information Technology, and he appointed a coordinator to serve as an advisor to the Secretary of Health and Human Services (HHS) and ensure coordination between HHS's health information technology initiatives and those of other federal agencies.[50] In doing so, the Bush administration established a ten-year plan for the implementation of a national, interoperable EHR system.[51] This Nationwide Health Information Network would be composed of linked Regional Health Information Organizations that would transmit patient data in EHRs to the physicians treating that patient.[52]

However, despite this initiative, the implementation of EHRs at the national and regional level has been mostly piecemeal, with different agencies and healthcare organizations developing electronic databases of patient information as part of their own programs. For example, the Health Resources Services Administration and several state agencies have worked to develop electronic child health profiles that link electronic medical records in individual healthcare providers' offices with community-based immunization registries.[53] In addition, several hospital systems have developed Regional Health Information Organizations that link patient medical records together within the hospital system or geographic area.[54] Insurance companies have also used similar systems to link International Classification of Diseases (ICD) codes[55] to electronic patient records in order to assess cost-effectiveness of EHRs and to explore ways to reduce medical errors.[56]

---

[49] *See* Medicare Prescription Drug, Improvement, and Modernization Act of 2003, Pub. L. No. 108–173, 117 Stat. 2066 (2003).

[50] GOV'T ACCOUNTABILITY OFFICE, *supra* note 48, at 14–15, *available at* http://www.gao.gov/new.items/d04991r.pdf.

[51] Laura Dunlop, *Electronic Health Records: Interoperability Challenges Patients' Right to Privacy*, 3 SHIDLER J. L. COM. & TECH. ¶ 1 (Apr. 6, 2007), http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/400/vol3_no4_art16.pdf?sequence=1.

[52] *Id.*

[53] David W. Hollar, *Progress Along Developmental Tracks for Electronic Health Records Implementation in the United States*, 7 HEALTH RES. POL'Y & SYS. 3, 4–5 (2009).

[54] *Id.* at 6–7.

[55] The ICD is the international standard diagnostic classification system used to classify diseases and other health conditions recorded in health records, death certificates, and other vital records.

At the state and local levels, efforts to create an interoperable EHR system mirror the activities at the national level.[57] Many states have introduced initiatives to expand the use of health information technology. According to the 2006 Third Annual Survey of Health Information Exchange Initiatives and Organizations, sponsored by the eHealth Initiative Foundations, 28 states had started planning for the use of health information technology, while an additional seven states had begun to implement this technology.[58] In most cases, a state's governor's office or department of health has coordinated these initiatives.[59]

Some states have concentrated their health information technology efforts on EHR adoption.[60] For example, in Arizona, then-Governor Janet Napolitano signed Executive Order 2005-25: Arizona Health-e Connection Roadmap in August of 2005.[61] This established a committee tasked with creating a plan for the adoption of a statewide EHR network, including the creation of a not-for-profit, public-private partnership to manage this network.[62] In addition, the Minnesota e-Health Initiative, another public-private partnership, has invested $1.3 million in a project to establish an EHR network in rural and underserved areas throughout the state.[63] Finally, as part of a several-year study of the practicality of EHR use in community medical practices, Massachusetts launched a pilot program to establish EHRs in community-based settings.[64]

Despite some progress in federal agencies and at the state level, little has been done in develop a national EHR system, and hospital systems have been slow to adopt this new technology. In the first nationally representative study of the prevalence of EHR use in hospitals, researchers from the Harvard School of Public Health, Massachusetts General Hospital, and George Washington University found that fewer than two percent of surveyed hospitals had implemented comprehensive

---

It is published by the World Health Organization. *International Classification of Diseases (ICD)*, WORLD HEALTH ORGANIZATION (2010), http://www.who.int/classifications/icd/en/index.html.

56 Hollar, *supra* note 53, at 8–9.

57 Dunlop, *supra* note 51, ¶ 10.

58 *Id.*

59 *Id.*

60 *Id.* ¶ 11.

61 *Id.*

62 *Id.*

63 *Id.*

64 *Massachusetts Takes a Giant Step Toward Electronic Health Records*, HEALTH INFO. & MGMT. SYS. (Oct. 5, 2006), http://www.himss.org/ASP/topics_News_item.asp?cid=65349&tid=9.

EHR databases. [65] Furthermore, fewer than eight percent of hospitals had even basic EMR systems in place.[66] These low rates of implementation are significant given that agencies and organizations at all levels of government have advocated for the adoption of a national EHR system in order to improve the coordination of medical care and decrease costs. Although the adoption of EHRs within a hospital system can improve quality of patient care, EHRs that can move between health care providers will be most useful for improving coordination of medical care. As the launch of French DMP approaches, the financial incentives available to physicians and other health care providers under the ARRA may provide the best opportunity for the United States to revisit these goals.

B. EHR DEVELOPMENT IN FRANCE

As in the United States, the government was the driving force behind EHR adoption in France. Although the French health care system was ranked first in the WHO study of health system performance because of its overall efficiency and fairness,[67] like the U.S. health care system, the French health care system suffered from inadequate communication between health care providers in hospitals and those working in private practice in the community.[68] Although informal referral networks exist between general practitioners, specialists, and hospitals, the lack of formal relationships between providers makes continuity of medical care difficult.[69]

In France, health care providers are usually private physicians with fee-for-service practices.[70] Unlike in the United States, French physicians do not act as gatekeepers who oversee a patient's medical care and determine whether they require a specialist.[71] Patients can choose providers and be reimbursed through their insurance.[72] All

---

[65] *See* Ashish K. Jha et al., *Use of Electronic Health Records in U.S. Hospitals*, 360 NEW ENG. J. MED. 1628, 1628 (2009).

[66] *Id.*

[67] *See* WORLD HEALTH ORG., THE WORLD HEALTH REPORT 2000—HEALTH SYSTEMS: IMPROVING PERFORMANCE (2000); GUSMANO, *supra* note 40, at 37.

[68] GUSMANO, *supra* note 40, at 37.

[69] *Id.*

[70] Victor G. Rodwin, *The Health Care System Under French National Health Insurance: Lessons for Health Reform in the United States*, 93 AM. J. PUB. HEALTH 31, 31–37 (2003).

[71] *Id.*

[72] *Id.*

individuals are automatically enrolled in a not-for-profit insurance fund based on their occupation, and most individuals also have supplemental health insurance.[73] The French national health insurance program is funded by employer and employee payroll taxes as well as a "general social contribution" that the French treasury collects on all earnings, including investment income.[74] The national health insurance contributes 79 percent toward personal health costs, while supplementary insurance covers approximately 8 percent.[75] Out-of-pocket expenditures are usually approximately 13 percent of total costs.[76]

Administrative details about an individual's care are maintained on a *Carte Vitale*, which essentially acts as an electronic health insurance card.[77] The *Carte Vitale* is a credit card-sized smartcard that contains demographic and insurance information about the cardholder.[78] The card does not contain any medical information.[79] The *Carte Vitale* is part of the *SESAM-Vitale* system, which connects health care professionals electronically with the national health insurance system.[80] *SESAM-Vitale* was created in order to provide electronic, rather than paper-based, insurance claims submissions, which has resulted in dramatic time and cost savings.[81] A health care provider initiates an electronic claim form using special *SESAM-Vitale* equipment at his workplace, and the claim is validated after the provider's smartcard and the patient's *Carte Vitale* are inserted into the equipment's smartcard reader.[82]

A similar procedure, also using the health care provider's smartcard and the patient's *Carte Vitale*, will allow providers to gain

---

[73] *See id.*

[74] GUSMANO, *supra* note 40, at 30.

[75] *Id.*

[76] *Id.* French national health insurance works similarly to the way Medicare works for the elderly in the U.S., but the insurance systems covers individuals of all ages. Almost all individuals purchase supplemental insurance, which is similar to Medigap, in order to reduce their out-of-pocket costs and cover extra expenses including dental and vision care. However, unlike Medicare, there are no deductibles. Instead, there are small co-payments, which are dismissed for those with chronic diseases.

[77] EHR-IMPLEMENT, *supra* note 24, at 11.

[78] *The SESAM-Vitale Program*, GIE SESAM-VITALE (Aug. 2009), http://www.sesam-vitale.fr/programme/programme_eng.asp; J. DAVID CUMMINS AND BERTRAND VENARD, HANDBOOK OF INTERNATIONAL INSURANCE: BETWEEN GLOBAL DYNAMICS AND LOCAL CONTINGENCIES 261 (2007).

[79] EHR-IMPLEMENT, *supra* note 24, at 11.

[80] *Id.*

[81] *The SESAM-Vitale Program*, GIE SESAM-VITALE (Aug. 2009), http://www.sesam-vitale.fr/programme/programme_eng.asp.

[82] *Id.*

access to a patient's DMP once the system has been launched.[83] The DMP was created as part of French health reform legislation in August 2004.[84] The concept of a longitudinal medical record was not new, as the *carnet de santé*, a paper booklet, had been mandatory for French children since 1945.[85] Furthermore, legislation in the 1990s attempted to create longitudinal paper medical records for all national health insurance beneficiaries over the age of 16, although privacy concerns ended these initiatives.[86] The concept was revived in 2003 because of sharp increases in medical costs as well as a growing awareness of the lack of coordination between hospitals and private physicians.[87] Thus, as part of an attempt to "implement a structural reform" of the health insurance system, the French government introduced the DMP as a way to improve coordination of health care.[88]

This project was perhaps too ambitious, as the law indicated that the DMP would be available for all national health insurance beneficiaries in 2007.[89] No studies had been conducted on the feasibility of the DMP, and health professionals, wary of the privacy concerns raised by the efforts to create longitudinal paper medical records in the 1990s, were concerned that the data contained in the DMP could be used for purposes other than coordinating a patient's care between providers.[90] Furthermore, the transition to electronic records, especially in hospitals, was still in the early stages.[91] As a result, the new Minister of Health, Roselyne Bachelot-Narquin, put the project on hiatus in 2008 in order to allow for time to study the feasibility of the DMP.[92]

After investigations conducted by the *inspectorate-general* of social affairs (IGAS) and the general council for information technologies (CGTI), Bachelot-Narquin announced in April 2009 that the DMP would be reexamined and that her office would be involved in supporting the needed changes.[93] The priorities of the new project include a simplification of the way in which public projects are managed

---

[83] EHR-IMPLEMENT, *supra* note 24, at 17.
[84] *See* ARTMANN & GIEST, *supra* note 27, at 16–17.
[85] EHR-IMPLEMENT, *supra* note 24, at 17.
[86] *Id.*
[87] *Id.* at 18.
[88] *Id.*
[89] *Id.* at 14.
[90] *Id.* at 18.
[91] *Id.*
[92] ASIP SANTÉ, *supra* note 28.
[93] *See id.*

and organized and the creation of regional health agencies, as well as a stronger focus on shared information systems.[94] The agency ASIP Santé was created to oversee this project, and this new version of the DMP was launched in 2010.[95]

Like all EHRs, the DMP contains all information and data deemed necessary for the coordination of a patient's care between providers. This information includes: demographic information, medical and surgical history, allergies and any chronic conditions, immunization history, results of laboratory tests, results of other diagnostic procedures, x-ray and MRI reports and images, and treatment information.[96] The data is organized by category in chronological order.[97] Information is entered by health care professionals who have been approved by the patient, and all providers will use health record software that is interoperable with the DMP.[98] All information must be dated and signed so that the author may be identified.[99]

The DMP also allows patients to take responsibility for their own health care. In particular, they consent to the creation of their record and control the conditions for accessing it.[100] European Union privacy laws[101] and Article L. 1110-4 of the French Public Health Code gives a patient the right to object to the exchange of the patient's health information between health professionals.[102] Therefore, patients may restrict some portions of their record from individual health care providers. For example, a patient could choose to prevent his dentist from accessing the section of his DMP that contains his immunization record. Associations that represent patients' interests, like the Commission Nationale Informatique (CNIL), are working closely with organizations of health care professionals in order to ensure that patient rights are protected

---

94 *Id.*

95 *Id.*

96 EHR-IMPLEMENT, *supra* note 24, at 16.

97 *Id.*

98 *Id.*

99 *Id.*

100 *Id.*

101 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 38, art. 14 (July 3, 1996), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:FULL:EN:PDF [hereinafter Directive 95/46/EC].

102 *Confidentialité des Données de Santé*, ASIP SANTÉ (June 17, 2010), http://esante.gouv.fr/en/juridique/confidentialite-des-donnees-de-sante.

during the construction of the DMP and all subsequent health information systems.[103] Specifically, these organizations, along with the French national insurance system, the CNIL and ASIP Santé, are working together to draft a guide to patient consent.[104]

II. BARRIERS TO EHR IMPLEMENTATION

Data privacy and security concerns have been one of the major barriers to the adoption of EHRs and the implementation of a national HIE in both countries. Other barriers include a lack of technology standards that can facilitate interoperability and cost of implementing such a system.[105] However, while France has comprehensive national medical privacy laws in place due to its membership in the European Union,[106] the United States has a complicated mix of federal and state privacy laws.[107] These laws are the largest barrier that the United States faces in attempting to facilitate EHR adoption and the development of the NHIN.[108]

A. MEDICAL PRIVACY LAWS IN THE UNITED STATES

The concept of the confidentiality of patient information is fundamental to the practice of medicine.[109] However, a patient's right to privacy comes from a number of legal sources. In 1965, the U.S. Supreme Court recognized a fundamental constitutional right to privacy

---

[103] *Id.*

[104] *Id.*

[105] Ashley Edwards et al., *Barriers to Cross-Institutional Health Information Exchange*, 24 J. HEALTH INFO. MGMT. 22, 24–25 (2010), http://www.himss.org/content/files/jhim/24-3/9_EDWARDS.pdf.

[106] *See infra* Part II.B.

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

[108] In the United States, several other statutory barriers exist, as well. For example, laws about fraud and abuse, antitrust, malpractice, and some state regulations may also affect the development of an EHR framework. Although some statutes, particularly those that address fraud and abuse, have been amended in recent years in order to allow exceptions for EHRs, these safe harbors are sometimes narrow and may not cover all possible ways in which EHRs may be implemented. Furthermore, confusion about any remaining limitations on EHRs imposed by these laws as well as state regulations that vary across the country has discouraged not only the use of EHRs by healthcare providers but also the development of a network that would facilitate sharing of EHR data. *See* James G. Anderson, *Social, Ethical, and Legal Barriers to E-Health*, 76 INT'L. J. MED. INFORMATICS 480, 481–82 (2007).

[109] Kathleen Knepper, *The Medical Records Maze: A Construct of Federal Inaction and State Inconsistency*, 31 J. HEALTH & HOSP. L. 114, 114 –115 (1998).

in *Griswold v. Connecticut*.[110] Some lower courts have suggested that the interest in maintaining control over one's personal medical records is rooted in constitutional privacy issues.[111] However, the Supreme Court held in *Whalen v. Roe* that while there may be a constitutional duty not to disclose personal information, state requirements regarding disclosure of private medical information to physicians and others did not violate patients' privacy interests per se.[112] The Court has not discussed whether a right to control the disclosure of information that is contained in an individual's medical records is a constitutional issue. Lacking constitutional control, medical privacy is generally protected by state and federal statutes.[113]

At the federal level, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) governs privacy of personal health information held by covered entities, which include health care providers, health plans, and health care clearinghouses.[114] The HIPAA Privacy Rule protects the privacy of individually identifiable health information by governing the internal use and external disclosure of protected health information (PHI).[115] The Privacy Rule established a set of basic national privacy standards that set minimum requirements for health care providers and health plans in order to protect patient privacy.[116] Under this Rule, a health care provider may use or disclose protected health information for the purposes of treatment, payment, or health care operations without patient consent.[117] The HIPAA Security Rule sets national standards for the security of electronic protected health information (PHI).[118] These standards create rules for when patient

---

[110] Griswold v. Connecticut, 381 U.S. 479, 485 (1965).

[111] *See* Amente v. Newman, 653 So. 2d 1030, 1033 (Fla. 1995); Mullins v. Griffin, 603 N.E.2d 1133, 1136 (Ohio Ct. App. 1991); *In re* June 1979 Allegheny County Investigating Grand Jury, 415 A.2d 73, 77–78 (Pa. 1980); Moses v. McWilliams, 549 A.2d 950, 954 (Pa. Super. Ct. 1988). *See also* People *ex rel.* Eichenberger v. Stockton Pregnancy Control Medical Clinic, Inc., 203 Cal.App.3d 225, 239 (Ct. App. 1988) (holding that minors have a right of privacy that protects information about their sexual experience and medical condition). *Contra* State *ex rel.* Stufflebam v. Appelquist, 694 S.W.2d 882, 885 (Mo. Ct. App. 1985) (holding that the physician-patient privilege has no constitutional basis).

[112] *See* Whalen v. Roe, 429 U.S. 589, 590–606 (1977).

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

[114] U.S. DEP'T OF HEALTH AND HUMAN SERVICES, SUMMARY OF THE HIPAA PRIVACY RULE 1 (2003), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

[115] *See* 45 C.F.R. §§ 160, 164.500–164.534 (2006).

[116] *Id.*

[117] *Id.*

[118] *See* 45 C.F.R. §§ 160, 164 (2002).

permission is required for use and disclosure, what that permission must contain, and how much of the PHI may be used or disclosed.[119] Finally, the Patient Safety Rule protects identifiable information from being used to analyze patient safety events and improve patient safety.[120]

The HIPAA Privacy Rule also created individual patient rights, some of which were new in many states.[121] These include the rights to: inspect and copy one's own PHI, amend erroneous or incomplete information, obtain an "accounting" of many disclosures of information, request restrictions of uses or disclosures for treatment, payment, or healthcare operations, receive confidential communications, and receive notice of a healthcare organization's privacy practices.[122] Further, the Privacy Rule establishes a number of administrative requirements, which mandate covered healthcare organizations to have an extensive set of policies to protect the privacy of health information, to appoint a "privacy official" to develop those policies, and to conduct workforce training on those policies.[123] Finally, these regulations govern communication with "business associates" to ensure that they also protect health information.[124]

Although HIPAA is an important source of patient privacy protection, it poses a challenge to the development of a national EHR system in the United States because of the ways in which it may conflict with state privacy laws, thus impeding progress toward the national goal of interoperability. In addition to federal privacy laws, some states, but not all, have adopted laws that govern the disclosure of medical records.[125] However, state laws are not consistent with one another, and they permit disclosure of medical information under different circumstances.[126] Therefore, as noted by one scholar, "to the extent that they exist at all, current patient access statutes lack the consistent scope and coverage necessary to protect effectively a patient's interests in the privacy and accuracy of her records."[127]

---

[119] 45 C.F.R. § 164.502 (2002).

[120] 42 C.F.R. pt. 3 (2009).

[121] *See* 45 C.F.R. § 164.506 (2003).

[122] *See id.*

[123] *Id.* at § 164.530.

[124] *Id.* at § 164.502(e)(1)(i).

[125] Knepper, *supra* note 109, at 119.

[126] *Id.*

[127] Ellen Klugman, *Toward a Uniform Right to Medical Records: A Proposal for a Model Patient Access and Information Practices Statute*, 30 U.C.L.A. L. REV. 1349, 1363 (1983).

In the absence of statutes that govern whether individuals have a right to privacy of their medical records in a particular situation, including state public records statutes and physician licensing requirements, courts have attempted to determine whether individuals have a common-law right to the confidentiality of their medical records.[128] Courts have usually found that the duty to protect the confidentiality of medical information is part of a physician's fiduciary duty to his patients; therefore, a breach of this duty is a tort.[129] Some courts have held that an implied contract is formed between a physician and a patient that prohibits a physician from disclosing medical information.[130]

Regardless of the source of a state's medical privacy law, the HIPAA Privacy Rule generally preempts state law when the state law is more lenient than these standards. That is, the Privacy Standards preempt state law when compliance with the state law would violate HIPAA.[131] However, there are several exceptions to HIPAA's preemption rule.[132] For example, state laws relating to the privacy of health information that are more favorable to patient privacy than the Privacy Standards are not preempted.[133] In addition, state laws governing public health surveillance, including the reporting of disease or injury, child abuse, birth, or death, or other investigations or interventions are allowed.[134] State laws that require health insurance plans to report information for the purpose of program monitoring and evaluation or audits are also permitted.[135] Finally, the Privacy Standards do not preempt state laws that relate to controlled substances or that the HHS Secretary deems necessary to prevent fraud and abuse, to ensure state regulation of insurance and health plans, or to serve a compelling public need related to public health, safety or welfare.[136]

Although the HITECH Act strengthened federal privacy law, the act does not address the conflict between federal and state privacy

---

[128] Knepper, *supra* note 109, at 120.

[129] *Id.*

[130] *Id.*

[131] 45 C.F.R. § 160.203 (2002).

[132] Beverly Cohen, *Reconciling the HIPAA Privacy Rule with State Laws Regulating Ex Parte Interviews of Plaintiffs' Treating Physicians: A Guide to Performing HIPAA Preemption Analysis*, 43 HOUS. L. REV. 1091, 1107 (2006).

[133] *Id.*

[134] *Id.*

[135] *Id.*

[136] *Id.*

laws.[137] Part D of the HITECH Act extends the privacy and security provisions of HIPAA to business associates of covered entities, including newly updated civil and criminal penalties.[138] Specifically, the law imposes new breach notification requirements on covered entities, business associates, vendors of personal health records, and other entities if a breach of PHI occurs.[139] The Department of Health and Human Services and the Federal Trade Commission have issued new regulations associated with the breach notification requirements.[140]

In addition, the HITECH Act updated the HIPAA rules for the accounting of PHI disclosures, including information used to carry out treatment, payment, and healthcare operations, so that they apply to the use of EHRs. [141] This requirement also limits the time frame for recording these disclosures.[142] However, it is still unclear how U.S. privacy law would govern a national HIE, because the interim rules that implement changes introduced by the HITECH Act have only recently gone into effect, and a "Final Rule" that will make changes to some HIPAA provisions is not expected until late June 2012.[143]

B. MEDICAL PRIVACY LAWS IN FRANCE

Like the United States, France has also had to address privacy concerns in its efforts to implement a nationwide health information network. As a member of the European Union, France must abide by

---

[137] *See* Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 115-5, § 13101, 123 Stat. 115, 92–101(2009). The purpose of this law was mostly to fund infrastructure development. *See id.*

[138] *Id.*

[139] *Id.*

[140] *See Breach Notification Final Rule Update*, U.S. DEP'T OF HEALTH AND HUMAN SERV., (July 28, 2010), http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/finalruleupdate.html; *see also FTC Issues Final Breach Notification Rule for Electronic Health Information*, FED. TRADE COMM'N (Aug. 17, 2009), http://www.ftc.gov/opa/2009/08/hbn.shtm.

[141] HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act, 76 Fed. Reg. 31, 426, 31, 426 (May 31, 2011), *available at* https://www.federalregister.gov/articles/2011/05/31/2011-13297/hipaa-privacy-rule-accounting-of-disclosures-under-the-health-information-technology-for-economic#p-3.

[142] *Id.*

[143] James B. Wieland, Sarah E. Swank & Joshua J. Freemire, *It's Coming: The HIPAA/HITECH Rule; What to Expect and What to do Now*, HEALTH L. ALERT (Ober|Kaler's: Attorneys at Law), no. 6, 2012, http://www.ober.com/publications/1781-its-coming-hipaa-hitech-rule-expect-do-now.

E.U. directives, including privacy laws.[144] Thus, France had comprehensive national privacy standards in place before beginning the DMP.[145] In France, the collection, use, and security of personal data are regulated by European Directive 95/46/EC[146] and a separate Act on Data Processing, Files, and Individual Liberties, which specifically addresses medical data.[147] Although the French Constitution of 1958 does not explicitly provide for a right to privacy, the Constitutional Council ruled that the Constitution implies a right to privacy.[148] The Council later confirmed this by explaining in 1999 that the freedom discussed in Article 2 of the 1789 Declaration of the Rights of Man and Citizen implies a right to privacy.[149] These E.U. privacy regulations broadly define personal data as "any information relating to an identified or identifiable natural person."[150] That is, data is personal when an individual can link the information to a specific person, like an address or a credit card number. Personal data should not be processed[151] unless the data subject has been informed,[152] and data processing is only allowed in limited circumstances, including when the data subject has given consent or when data processing is necessary to protect the vital interests

---

[144] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, ch. 1, art. 4, 1995 O.J. L 281. This directive requires each member state to enact its own local legislation adopting the directive. *Id.*

[145] *See supra* Part I.B. The DMP was created as part of French health reform legislation in August 2004 and reintroduced in 2009. Data privacy standards in France are governed by European Directive 95/46/EC, which was adopted in 1995. *See* Directive 95/46/EC, *supra* note 101, at 31.

[146] See *Directive 95/46/EC*, *supra* note 145, at 31.

[147] Commission nationale de l'informatique et des libertés, *Decree No 2005-1309 of 20 October 2005 Enacted for the Application of Act No 78-17 of 6 January 1978 on Data Processing, Files and Individual Liberties*, at art. 41 (2007), http://www.cnil.fr/fileadmin/documents/en/Decree%202005-1309.pdf.

[148] Conseil constitutionnel [CC] [Constitutional Court] decision No. 94-352 DC, Jan. 18, 1995, ¶ 2, *available at* http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/depuis-1958/decisions-par-date/1995/94-352-dc/decision-n-94-352-dc-du-18-janvier-1995.10612.html.

[149] Conseil constitutionnel [CC] [Constitutional Court] decision No. 99-416 DC, Jul. 23, 1999, ¶ 45, *available at* http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/1999/99-416-dc/decision-n-99-416-dc-du-23-juillet-1999.11847.html.

[150] *Directive 95/46/EC*, supra *note 145*, *art. 2*.

[151] The concept of *processing* refers to "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. Directive 95/46/EC, *supra* note 101, art. 2(b).

[152] *Id.* art. 10–11.

of the data subject.[153] The data subject has the right to be informed when his personal data is being processed,[154] and any actions taken with the data must be relevant to the purpose of the processing.[155] Extra restrictions apply to sensitive personal data, including religious beliefs, health, sexual orientation, and race.[156] Finally, each E.U. member state must establish an independent authority to monitor the data protection in that country, advise the government about privacy regulations, and initiate legal proceedings when a regulation has been violated.[157]

III. ADDRESSING BARRIERS TO EHR IMPLEMENTATION

A. BOTH COUNTRIES HAVE SUCCESSFULLY ADDRESSED SOME BARRIERS.

1. COST

The United States and France have both taken steps to address the financial and technological barriers to EHR adoption. In France, the DMP has been financed by the government, in anticipation of the amount of money the DMP will save in health care expenditures, as well as advertising and partnership arrangements.[158] In the United States, financial incentives will be provided to health care providers through the Medicare and Medicaid programs in order to offset the costs of adopting EHR technology.

In the United States, the Medicare EHR Incentive Program will provide incentive payments to eligible health care professionals, eligible hospitals, and critical access hospitals that demonstrate "meaningful use" of certified EHR technology.[159] Beginning in 2011, eligible professionals

---

[153] *Id.* art. 7.

[154] *Id.* art. 10–11.

[155] *Id.* art. 6.

[156] *Id.* art. 8.

[157] *Id.* art. 28.

[158] J. ARTMANN & S. GIEST, EUROPEAN COMMISSION, COUNTRY BRIEF: FRANCE 34 (2010), http://ehealth-strategies.eu/database/documents/France_CountryBrief_eHStrategies.pdf; Dossier Santé Personnel, *FAQ Dossier Médical (DSP)*, DOSSIER SANTÉ PERSONNEL (May 24, 2011), http://www.dossiersantepersonnel.com/dossier-medical/contenu.aspx?id_contenu=7 ("Le Dossier Santé Personnel se finance grâce à de la publicité et à des accords de partenariat.").

[159] CENTERS FOR MEDICARE & MEDICAID SERVICES, OFFICE OF PUBLIC AFFAIRS, *CMS EHR Meaningful Use Overview*, https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html. Interpreting the meaning of

can receive up to $44,000 over five years under this program, with an additional incentive provided for eligible professionals who provide services in a Health Professional Shortage Area.[160] Incentive payments for eligible hospitals are based on a number of factors, beginning with a $2 million base payment.[161] However, if Medicare eligible professionals and hospitals do not successfully demonstrate meaningful use, they will be reimbursed at a lower rate.[162]

Under the Medicaid EHR incentive program, eligible professionals and hospitals who adopt, implement, upgrade, or demonstrate meaningful use of certified EHR technology in their first year of participation and demonstrate meaningful use for up to five years will receive incentives.[163] Eligible professionals may receive up to $63,750, while hospital payments are based on a number of factors, beginning with a $2 million base payment.[164] This program is voluntarily offered by individual states and territories.[165]

2. TECHNOLOGICAL BARRIERS

In the United States, the Office of the National Coordinator (ONC) for Health Information Technology and the Centers for Medicare & Medicaid Services have adopted standards, implementation specifications, and certification criteria for EHR technology.[166] In order for a provider to qualify for EHR incentive payments for meaningful use,

---

"meaningful use" is a challenge for hospitals and other health care professionals. The ARRA defines three main components of meaningful use: (1) The use of a certified EHR in a meaningful manner, such as e-prescribing; (2) The use of certified EHR technology for electronic exchange of health information to improve quality of health care; and (3) The use of certified EHR technology to submit clinical quality and other measures. In general, "meaningful use" means providers must show that they're using EHR technology in ways that can be measured quantitatively and qualitatively. *Id.*

[160] CMS OFFICE OF PUBLIC AFFAIRS, *Fact Sheet: CMS Finalizes Definition of Meaningful Use of Certified Electronic Health Records (EHR) Technology*, 1 (July 16, 2010), *available at* https://www.cms.gov/apps/media/press/factsheet.asp?Counter=3792&intNumPerPage=10&checkDate=&checkKey=&srchType=1&numDays=3500&srchOpt=0&srchData=&keywordType=All&chkNewsType=6&intPage=&showAll=&pYear=&year=&desc=&cboOrder=date.

[161] *Id.*

[162] *Id.*

[163] *Id.*

[164] *Id.*

[165] CENTERS FOR MEDICARE & MEDICAID SERVICES, OFFICE OF PUBLIC AFFAIRS, *Medicaid State Information*, https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/MedicaidStateInfo.html

[166] CENTERS FOR MEDICARE & MEDICAID SERVICES, *Certified EHR Technology* (Oct. 11, 2011), https://www.cms.gov/EHRIncentivePrograms/25_Certification.asp.

EHR software used must be tested and certified by an ONC Authorized Testing and Certification Body.[167] According to the ONC, certified EHR technology is "[a] [c]omplete EHR or a combination of EHR Modules, each of which (1) meets the requirements included in the definition of a Qualified EHR; and (2) has been tested and certified in accordance with the certification program established by the National Coordinator as having met all applicable certification criteria adopted by the [ONC]."[168] By encouraging health care providers to adopt only EHRs that meet specific national standards, the government is preparing for the eventual implementation of the NHIN.

Similarly, the French government has adopted software standards in order to ensure that different providers using different software platforms will still be able to view all patient data that has been entered.[169] Ideally, DMP software should be developed in such a way that it interfaces with existing software used in the clinical setting so that data transmission from the existing software happens automatically.[170] Within the DMP, documents are tagged in such a way as to facilitate grouping by type of document or in chronological order, if desired.[171] Setting standards that streamline the data transfer process facilitates true interoperability of the system.

B. FRANCE'S APPROACH TO ADDRESSING DATA PRIVACY CONCERNS COULD SERVE AS AN EXAMPLE FOR THE U.S.

In order for a national HIE to be successful, the United States must adopt a uniform national privacy law. If, for example, the HIPAA Privacy Rule, without HIPAA's preemption provisions, served as the uniform standard for confidentiality of medical data, the United States could quickly achieve widespread and meaningful use of EHRs, meaning that providers would be using certified EHR technology in measurable

---

[167] *Id.*

[168] Chris Thorman, *Updates on Meaningful Use, Certified EHR Technology, and the Stimulus Bill*, HEALTHCARE IT NEWS (Feb. 4, 2010), http://www.healthcareitnews.com/blog/updates-meaningful-use-certified-ehr-technology-and-stimulus-bill.

[169] ASIP SANTÉ, *The Interoperability Framework: a Modular, Continuously Evolving Foundation* (June 21, 2010), http://esante.gouv.fr/en/dossiers/interoperability-framework-a-modular-continuously-evolving-foundation.

[170] EHR-IMPLEMENT, *supra* note 24, at 16.

[171] *Id.*

ways.[172] Unfortunately, as discussed above, exceptions to HIPAA's preemption provision will make it difficult for health care providers to share patient health information across state lines.[173] Thus, a single Federal privacy rule that sets consistent national data security standards for medical information would end confusion about which statutes govern a particular disclosure of protected health information.

Under HIPAA as it would exist without exceptions to the preemption provision, EHRs would make it possible for all health care providers who may be consulted about a specific patient's care to have access to that individual's health records from all current and past providers.[174] This means that any health care provider would have access to an individual's entire health record from his birth to his most recent encounter with the health care system.[175] This access would not require patient consent because, under the HIPAA Privacy Rule, disclosures of protected health information for treatment purposes do not require authorization.[176]

However, if people fear that their medical information will be disclosed to any health care provider who may treat them at some point during their lives, they might fail to divulge sensitive information relevant to their care, make up answers to sensitive questions, or even avoid seeking care altogether, potentially harming their own health or the health and safety of others.[177] To this end, the NCVHS has recommended that HHS adopt a policy for the NHIN that would allow individuals to have limited control over the disclosure of sensitive health information in their records.[178] This policy would resemble Article L. 1110-4 of the French Public Health Code, which gives a patient the right to object to the exchange of the patient's health information between health professionals.[179] Thus, French patients are able to restrict some portions of their DMP from individual health care providers.

---

[172] *See* Stephen J. Weiser, *Breaking Down the Federal and State Barriers Preventing the Implementation of Accurate, Reliable and Cost Effective Electronic Health Records*, 19 ANN. HEALTH L. 205 (2010). For more information about meaningful use, see *supra* note 159.

[173] *See supra* p. 24.

[174] Letter from Simon P. Cohn, Chairman, National Committee on Vital and Health Statistics, to Michael O. Leavitt, Secretary, U.S. Department of Health and Human Services (Feb. 20, 2008), *available at* http://www.ncvhs.hhs.gov/080220lt.pdf [hereinafter NCVHS Letter].

[175] *Id.*

[176] *Id.*

[177] *Id.*

[178] *Id.*

[179] *See supra* Part I.B.

NCVHS recommended that health care providers be notified that some information in a patient's record has been withheld at the patient's request.[180] Because patients can currently choose not to tell a provider about health information, a notation in a patient's EHR that information has been withheld may actually reveal more information than is available today.[181] However, such a notification could also serve to increase providers' trust in the accuracy of the record.[182] If providers knew that patients could withhold sensitive information, they could never be sure that records were complete.[183] The notification that information is missing gives a provider the opportunity to discuss with a patient the concerns about the missing information and its possible effect on care.[184]

NCVHS suggested two possible ways in which providers could be notified that information is missing. One approach would be to alert a provider that some information has been withheld without providing any indication of the category of information that is missing.[185] Because the nature of a particular category of sensitive information might reveal more than the patient wishes to disclose, this approach may increase patient privacy.[186] Although a provider might not need to see the information for routine care, the provider may feel required to question patients about categories of missing information in order to determine whether the withheld information is relevant.[187] This could ultimately make the system less efficient and less protective of patient privacy.[188]

A second approach to notifying providers that information is missing would involve letting a provider know which category of information has been withheld.[189] This allows the provider to determine whether the information may be relevant to the current visit without asking the patient.[190] A disadvantage of this approach is that some categories, by themselves, reveal information that has been withheld, such as whether a patient has a mental health condition or a history of substance abuse. In situations like this, designations of specific

---

[180] NCVHS Letter, *supra* note 174.
[181] *Id.*
[182] *Id.*
[183] *Id.*
[184] *Id.*
[185] *Id.*
[186] *Id.*
[187] *Id.*
[188] *Id.*
[189] *Id.*
[190] *Id.*

categories of sequestered information might not adequately protect patient privacy.[191] However, this approach has the potential to be more efficient, and, since most of the time sequestered information would remain hidden, it could adequately protect the patient's privacy.[192]

In situations where a patient may be unable to give or refuse consent to the disclosure of sensitive health information, such as when a patient is unconscious, a physician may need to access the patient's full record in order to determine whether any information that has been withheld is relevant to the current situation.[193] NCVHS has recommended that a feature be put in place that allows a provider to access the patient's complete health information in an emergency.[194] Such a feature would include an audit trail in order to record the details of the incident and could also prompt a review by a privacy officer. Furthermore, the patient or a representative of the patient would be notified as soon as possible that the full record had been disclosed.[195] This feature would be consistent with the concept of implied consent to treat an individual in an emergency and would protect the strong public interest in providing necessary treatment.[196] Finally, any information that had previously been withheld would be unavailable to the provider once the emergency was over.[197]

The NCVHS recommendations were based on the following considerations: protecting patients' legitimate concerns about privacy and confidentiality, fostering trust, and encouraging participation in the NHIN in order to promote opportunities to improve patient care, and protecting the integrity of the health care system.[198] These recommendations resemble the control that French patients have been given over their DMP and should be piloted in states with advanced regional health information networks already in place in order to identify the best strategies for developing a national system. Implementing these suggestions should allow the NHIN to be efficient and affordable, while still protecting the confidentiality of patient information.[199]

---

[191] *Id.*
[192] *Id.*
[193] *Id.*
[194] *Id.*
[195] *Id.*
[196] *Id.*
[197] *Id.*
[198] *Id.*
[199] *Id.*

CONCLUSION

Although the initial push for national HIE development and implementation in the United States and France began around the same time, the United States has lagged behind France in its attempts to build a national EHR framework. In both countries, a national HIE is seen as a way to improve coordination of medical care while decreasing costs.[200] While both countries have addressed the organizational and technological requirements for implementation of a national EHR system, a complex patchwork of privacy laws in the United States pose an enormous legal challenge to the implementation of a national HIE. In order to implement the NHIN successfully, the United States must reexamine these laws in order to ensure that they are compatible with national health information technology goals. That is, successful adoption of a national HIE requires the development of a comprehensive national privacy law, perhaps similar to French privacy laws, that allows for the exchange of health information between providers while still protecting patient privacy. Furthermore, stakeholders, including providers and patients, must be educated about any actual limitations imposed by these and any other laws that govern EHR adoption in order to alleviate confusion. Once these barriers have been lifted, the United States will be able to develop a more comprehensive plan for a national EHR network.

[200] *See supra* Introduction.