Interoperable Electronic Healthcare Record: A Case For Adoption Of A National Standard To Stem The Ongoing Healthcare Crisis

Deth Sao
Amar Gupta
David A. Gantz

Available at: http://works.bepress.com/deth_sao/6/
INTEROPERABLE ELECTRONIC HEALTHCARE RECORD: A CASE FOR ADOPTION OF A NATIONAL STANDARD TO STEM THE ONGOING HEALTHCARE CRISIS.

Deth Sao
J.D. 2010, James E. Rogers College of Law, University of Arizona; B.A. 2001 Wellesley College; of the Massachusetts and New York Bars.

Amar Gupta
Thomas R. Brown Endowed Professor, Eller College of Management, University of Arizona; concurrent appointments in the College of Science, College of Public Health, College of Social and Behavioral Sciences, Rogers College of Law, and the College of Pharmacy (HOPE Center); Ph.D. 1980, Indian Institute of Technology Delhi; M.S. 1980, Massachusetts Institute of Technology Sloan School of Management; Bachelor of Technology 1974, Indian Institute of Technology Kanpur.

David A. Gantz
ABSTRACT

Interoperable electronic health records (EHR) have the capacity to deliver health care at optimal costs and quality in the United States, but current private and public initiatives have delayed nationwide implementation by failing to overcome several obstacles. These obstacles include: widespread reluctance in adopting health information technology (HIT); differing technical and semantic standards for communication between vendor systems; and legal challenges, which are mainly based on liability, privacy, and security concerns. This paper examines these challenges and the inadequacies of current HIT-EHR implementation strategies, questioning in particular the validity of privacy and security-based concerns. A comparison with the U.S. finance industry and other nations facing similar challenges not only undermine these concerns, but also point to pursuit of revolutionary solutions when traditional approaches fail. To efficiently and effectively facilitate the development of interoperable EHRs and help stem the crisis of rising costs and discontent in the U.S. healthcare sector, this paper proposes enactment of federal legislation mandating uniform technical standards to maintain and transfer health records as a necessary first step and integral part of a successful solution.

I. INTRODUCTION

In less than a decade, the United State’s Department of Veterans Affairs (VA) transformed its image from a healthcare provider of last resort to the best healthcare provider in the nation.¹ Plagued by a “tarnished reputation of bureaucracy, inefficiency, and mediocre care,”² the VA sought to reinvent itself by implementing structural, organizational, and technological changes in the mid-1990s.³ A key contributor to the VA’s swift and far reaching success lies in its adoption of a comprehensive electronic medical record (EMR) infrastructure,⁴

² PERLIN, KOLDNER & ROSWELL, supra note 1, at 11. The VA suffered from this reputation throughout the 1980’s and early 1990’s. Id.
³ Id. at 17, 22-23 (noting that in combination with performance management and patient centric focus, the VA’s EHR system has enabled VA to provide more effective health care).
⁴
a computerized database enabling instant access to patient records across all VA and Department of Defense treatment facilities nationwide.\(^5\) Touted as the “most extensive [EMR] system in the U.S.,”\(^6\) it provides 100% patient record availability and incorporates extensive administrative and clinical capabilities to facilitate, track, and monitor patient care\(^7\) across 163 hospitals, 800 clinics, and 135 nursing homes.\(^8\)

By the mid-2000’s, the VA’s EMR system was widely praised for its crucial role in establishing the VA as the best U.S. healthcare provider in many performance areas. Several of these successful applications include:

- use of computerized provider order entry that decreased rates of adverse drug events\(^9\) and increased prescription accuracy rates to greater than 99.997%, in comparison to the national 3-8% error rate;\(^10\)

- providing the highest quality of care nationally for almost all conditions as a result of performance measurement systems tracking patient data;\(^11\) and

- stabilization in costs per patient despite increasing price inflation, which is largely attributed to the elimination of repetitive lab tests and paperwork.\(^12\)

Utilized in tandem with coordinated health care and accountability strategies, such applications have enabled the VA to provide two-thirds of care recommended by national standards in comparison to half provided nationally.\(^13\)

---

\(^5\) Id. at 18.
\(^6\) Arnst, supra note 1.
\(^7\) PERLIN, KOLDNER & ROSWELL, supra note 1, at 17, 22-23; Arnst, supra note 1. Administrative and clinical capabilities include: computerized provider order entry, critical alerts, and a clinical reminder system to provide real-time decision report. For more information, see generally, PERLIN, KOLDNER & ROSWELL, supra note 1.
\(^9\) PERLIN, KOLDNER & ROSWELL, supra note 1, at 17.
\(^10\) Arnst, supra note 1.
\(^11\) The VA outperforms its counterparts in a national sample in all care categories except for acute care, where VA results were similar to the national sample. ASCH ET AL., supra note 1, at 2.
\(^12\) Arnst, supra note 1.
\(^13\) ASCH ET AL., supra note 1, at 1-2.
The VA’s success demonstrates the capacity of healthcare information technology (HIT) to deliver medical services at optimal costs and quality. Several countries have harnessed this capacity on a vastly greater scale by implementing an electronic health record (EHR) infrastructure, a nationwide network that goes beyond communications within one healthcare entity to enable sharing of patient data among numerous healthcare entities. In comparison, the U.S. is far from reaching this goal. While there is a general consensus among U.S. healthcare policymakers and legislators on the benefits and necessity of an HIT-EHR framework, the following obstacles have delayed its adoption: a low adoption rate of HIT nationwide; a plethora of differing technical standards for communication between vendor systems, thereby preventing interoperability among these disparate systems; and legal challenges, which are mainly based on liability, privacy, and security concerns. This paper examines these challenges and existing initiatives to overcome these challenges, and proposes enactment of federal legislation mandating uniform technical standards to maintain and transfer health records as an integral part of an effective solution. Part II discusses the potential of HIT-EHR to play a key role in resolving the ongoing healthcare crisis in the U.S. Part III analyzes barriers to HIT-EHR development, assessing in particular the validity of privacy and security-based concerns among the healthcare community and consumers. The legitimacy of such concerns is undermined when compared with the finance industry, which shoulders similar privacy and security challenges and

---

17 ARNOLD ET. AL., supra note 14, at 5.
18 John R. Christiansen, Legal Speed Bumps on the Road to Health Information Exchange, 1 J. HEALTH & LIFE SCI. L. 1, 20 (2008).
successfully operates on national and global levels. Part IV discusses the inadequacies of current private and public initiatives intended to facilitate HIT-EHR development. Finally, Part V argues for the enactment of federal legislation mandating uniform technical standards as a necessary first step towards efficient and widespread HIT-EHR implementation.

I. THE POTENTIAL OF AN HIT-EHR FRAMEWORK

As illustrated by the VA’s experience, the implementation of an HIT-EHR infrastructure would make significant inroads in resolving the ongoing U.S. healthcare crisis by dramatically reducing costs and improving the quality of care. In an era where participants and services in the healthcare industry intersect on national and global levels, an EHR’s accessibility and versatility enables healthcare providers to achieve these benefits. Unlike an EMR, which are computerized patient records maintained within a single healthcare entity (such as the VA), an EHR is an electronic record of a patient’s medical history made available nationally regardless of where a patient receives diagnosis and treatment. An EHR combines detailed information from all healthcare entities that have provided medical services to the patient in question. By enabling greater access to and offering a platform to monitor and analyze such comprehensive data, EHRs have the potential to concurrently improve the quality of care and reduce billions in costs annually.

A. An HIT-EHR Infrastructure May Significantly Reduce Healthcare Costs

Estimates range from $77.8 to $162 billion in cost savings per year in the U.S. by streamlining administrative procedures and eliminating redundant diagnostic tests and

---

20 Id. at ¶ 4.
paperwork.\textsuperscript{22} U.S. administrative expenses absorb an estimated 31% of total U.S. healthcare costs, which are approximately 30-70% higher than comparable countries with mixed public-private systems.\textsuperscript{23} The use of EHRs would reduce administrative tasks by accelerating information transfers.\textsuperscript{24} Additionally, such swift data exchanges would greatly reduce repetitive tests and paperwork conducted as a result of misplaced or unavailable records.\textsuperscript{25} Finally, EHR makes available the option to outsource and offshore medical and nonmedical services – strategies that will increase efficient delivery of health care at optimal prices.\textsuperscript{26}

B. An HIT-EHR Infrastructure May Improve the Quality of Care

EHR provision of instant access to comprehensive accounts of patients’ medical histories enables healthcare providers to improve the quality of care in several ways. First, unlike paper records, EHRs enable portability and simultaneous viewing by multiple users\textsuperscript{27} – features which are indispensable for uninterrupted treatment of patients who are mobile or displaced as a result of a crisis. For instance, VA patients were the only ones whose medical records were immediately available following the evacuation of New Orleans hospitals during Hurricane Katrina.\textsuperscript{28} Second, clarity of records helps prevent medical and medication errors.\textsuperscript{29} Because many medical errors arise from handling of paper-based records, transference to an electronic platform would dramatically reduce manual mistakes by avoiding errors such as mislabeling,

\textsuperscript{22} Id. at 5; Ariele Yaffee, \textit{Financing The Pulp To Digital Phenomenon}, 7 J. HEALTH & BIOMEDICAL L. 325, 332-33(2011).
\textsuperscript{23} This estimate includes administrative costs of hospitals, doctors, insurers, and government. WULSIN & DOUGHERTY, \textit{supra} note 8, at 1.
\textsuperscript{24} Id. at 4.
\textsuperscript{25} Id.
\textsuperscript{28} Arnst, \textit{supra} note 1.
\textsuperscript{29} Terry & Francis, \textit{supra} note 15, at 683.
mishandling requests, or misfiled or missing information.\textsuperscript{30} A clear and organized record format further enables clinicians to readily respond to relevant information and catch errors and issue advice and warnings when inadequate treatment is identified.\textsuperscript{31} Third, EHRs allows tracking and analysis of data in order to more effectively treat patients and determine areas of strength and weakness. Examples include identifying patterns for diseases, prescription use, and inadequate treatment strategies.\textsuperscript{32} Instant and updated access to data among multiple healthcare providers further enables patients to reap the full benefits of coordinated care.\textsuperscript{33} Finally, EHRs offer the promise of improving delivery of health care on a global level. Potential scenarios of coordinated care include global monitoring of safety of medicines and online access for professionals and patients to updated information on every specialty.\textsuperscript{34}

\textbf{II. BARRIERS TO NATIONAL HIT-EHR IMPLEMENTATION}

The full realization of an HIT-EHR framework is impeded by a severely underdeveloped infrastructure and widespread concerns among the healthcare community and consumers surrounding privacy and security safeguards. As the analysis below discusses, the low adoption rate of HIT nationwide results in a sporadic and weak foundation for EHR development while the plethora of HIT vendors obstruct data transfers due to the incompatibility of their systems. Just as problematic is the pervasive presumption among the public and stakeholders that HIT-EHR poses new and greater privacy and security risks and thus, should be abandoned or delayed until these risks are resolved. While a comprehensive legal framework resolving privacy and security breaches is lacking and must be developed, fears that HIT-EHR itself automatically

\textsuperscript{30} Yaffee, supra note 22, at 335.
\textsuperscript{31} Barrows & Clayton, supra note 27, at 147.
\textsuperscript{32} Terry & Francis, supra note 15, at 683.
\textsuperscript{33} Id.
\textsuperscript{34} Gupta, supra note 26, at ¶ 4.
results in increased and inevitable breaches are misguided. Such challenges will always be ongoing and in varying degrees whether health information is stored in paper or electronic format. Just as importantly, such fears defy the reality of existing HIT-EHR operating successfully with appropriate security safeguards in place.\textsuperscript{35} Furthermore, the experience of the finance industry on national and global levels underscores these observations, as it has dramatically improved its business processes utilizing IT processes but must continually adapt and respond to similar privacy and security concerns surrounding personal financial information.

A. Infrastructural Challenges: HIT-EHR is Underdeveloped in the United States

Many industrialized nations have pursued and benefited by widespread HIT adoption, with approximately 80-100\% of healthcare providers utilizing EMR systems.\textsuperscript{36} In comparison, the U.S. healthcare sector has been slow to adopt and maximize information systems and capabilities.\textsuperscript{37} Presently, only 15-20\% of physicians’ offices and 20-25\% of hospitals have EMR systems in place.\textsuperscript{38} The few equipped with EMR systems fail to reap the full benefits of such technology through lack of interoperability, which is defined as “the ability of two or more systems or their components to exchange information and to use the information that has been exchanged.”\textsuperscript{39} The large number and variety of information systems have given rise to different rules and formats for maintaining and transferring patient data, thereby obstructing data


\textsuperscript{36} Yaffee, \textit{supra} note 22, at 332-33.

\textsuperscript{37} \textit{See ARNOLD ET. AL., supra} note 14, at 1.


\textsuperscript{39} \textit{HIMSS, INTEROPERABILITY DEFINITION AND BACKGROUND} 2 (2005), http://www.himss.org/content/files/interoperability_definition_background_060905.pdf.
Without uniform communication protocols for data transmission among systems, specifically defined as technical interoperability, it is impossible to share data among healthcare entities and often among units within a single entity. Differences in technical standards include variations in languages and measures and conflicts between encryption and other software. As a result, these disparate EMR systems are underutilized by solely functioning as isolated islands of information.

A major contributor to reluctance of the U.S. healthcare community in investing in HIT-EHR is largely attributed to considerable implementation costs and the uncertainty among healthcare providers over whether they would ultimately financially benefit. Cost considerations have the greatest impact on small hospitals and practices, as they most likely lack sufficient capital for such an investment. For example, a small hospital pays an estimated three million U.S. dollars for HIT-EHR implementation. Medicare and Medicaid incentives cover approximately 47-67% of HIT-EHR adoption costs, with the average cost to an eligible healthcare provider amounting to $94,000 over the course of five years.

As to the question of whether HIT-EHR will enable healthcare providers to make worthwhile monetary returns on such an investment, the benefits are difficult to quantify. Traditional cost and reimbursement models for healthcare financing assign implementation and maintenance costs to healthcare providers while insurers and payors are the recipients of

---

40 Gupta, supra note 26, at ¶ 18.
41 Baird, supra note 16, at 231-32.
42 See Gupta et al., supra note 21, at 6-7.
43 Gupta, supra note 26, at ¶ 18.
44 Yaffee, supra note 22, at 349.
45 WULSIN & DOUGHERTY, supra note 8, at 9.
46 Yaffee, supra note 22, at 349.
47 Id. at 350.
48 Id.
resulting cost savings.\textsuperscript{49} Healthcare providers must take on costly and time consuming responsibilities such as personnel training and equipment purchases.\textsuperscript{50} The resulting increases in quality of care arguably cut into profits, as there would be less utilization of health services.\textsuperscript{51} As a result, healthcare providers have been reluctant to invest in a product that incurs great expense without any seemingly upfront or clear measurable benefits.\textsuperscript{52}

**B. Privacy, Security, and Liability Concerns**

Delayed adoption of HIT-EHR is also attributed to widespread concerns over (1) increased exposure to legal uncertainty and compliance costs surrounding privacy and security breaches\textsuperscript{53} and (2) excessive fears that HIT-EHR will lead to unmanageable and automatic privacy and security breaches.\textsuperscript{54} HIT-EHR data storage and transfer capabilities create new avenues for unauthorized access to and misuse of health information.\textsuperscript{55} While the fragmented U.S. legal landscape justifies concerns of legal uncertainty and costly compliance costs, the availability and use of HIT-EHR security safeguards and comparisons to the finance industry undermine the validity of fears regarding HIT-EHR use.

1. **Legal Challenges**

Areas of overlap and inadequacy in federal and state laws and regulations incur higher costs in HIT-HER implementation in order to ensure compliance.\textsuperscript{56} The 1996 Health Insurance Portability and Accountability Act (HIPAA) sets forth requirements at the federal level,\textsuperscript{57} but its effectiveness is limited by its narrow scope, ambiguous and confusing guidelines, and deference

\textsuperscript{49} Wulsin & Dougherty, * supra* note 8, at 9.
\textsuperscript{50} Id.
\textsuperscript{51} Id.
\textsuperscript{52} Id.
\textsuperscript{53} Yaffee, * supra* note 22, at 344.
\textsuperscript{54} Gantz, * supra* note 35.
\textsuperscript{55} Yaffee, * supra* note 22, at 343.
\textsuperscript{56} Christiansen, * supra* note 18, at 27.
\textsuperscript{57} 42 U.S.C. § 1320(d) to (d)-8 (2000).
to state laws that do not conflict and are more strict.\textsuperscript{58} Subsequent federal legislation, namely the Health Information Technology for Economic and Clinical Health Act (HITECH Act) under American Recovery and Reinvestment Act of 2009, has made strides in correcting HIPPA’s weaknesses.\textsuperscript{59} However, these recent measures still fall short of comprehensive and uniform legislation needed in this area.\textsuperscript{60} These compliance issues are analyzed below.

a. Privacy and Security Considerations

An HIT-EHR framework implicates privacy and security concerns because electronic storage and transfer of health information among numerous computer servers exposes data to privacy and security breaches and human error.\textsuperscript{61} Existing federal and state laws and regulations offer no clarity on standards or protocols for compliance. With regards to security, HIPAA mandates covered entities to establish safeguards tailored to their own organization’s needs.\textsuperscript{62} State laws fail to provide better guidance, as few states have updated their security laws to address electronic transfers of health information.\textsuperscript{63} With regards to privacy, HIPAA confidentiality regulations are unclear and fail to provide adequate private protections.\textsuperscript{64} Major dilemmas include: lack of standards for patient consent; uncertainty over whether secondary uses may be controlled in the context of a national HIT-EHR framework;\textsuperscript{65} and confusion regarding the appropriate level of patients’ input in permissible uses of their health information.\textsuperscript{66}

\textsuperscript{58} 42 U.S.C. § 1320d-2; see 63 Fed. Reg. at 43,258; see Christiansen, \textit{supra} note 18, at 24.
\textsuperscript{59} Yaffee, \textit{supra} note 22, at 331.
\textsuperscript{60} \textit{See} Christiansen, \textit{supra} note 18, at 22.
\textsuperscript{61} Dunlop, \textit{supra} note 19, at ¶7.
\textsuperscript{62} Christiansen, \textit{supra} note 18, at 23.
\textsuperscript{63} \textit{Id. } at 25.
\textsuperscript{64} Terry & Francis, \textit{supra} note 15, at 683.
\textsuperscript{65} Christiansen, \textit{supra} note 18, at 22.
\textsuperscript{66} \textit{Id. } at 22-23.
Additionally, state laws and regulations contribute to such ambiguity by applying different laws to different categories of information and entity.\textsuperscript{67}

Under subsequent enactment of ARRA, the HITECH Act appointed the Department of Health and Human Services (HHS) to buttress these weaknesses in HIPAA’s privacy and security guidelines.\textsuperscript{68} Examples of security enhancements include express and more stringent security breach notice requirements for covered entities and their business associates,\textsuperscript{69} as well as vendors of personal health records and vendors’ third party processors.\textsuperscript{70} With regards to stronger privacy provisions, covered entities and business associates must: (1) handle health information such that all personal identifiers are removed to the greatest extent possible, with the HHS determining when that threshold is met; (2) obtain valid authorization from patients in order to financially benefit from exchange of health information, except under certain exceptions; and (3) make efforts to resolve any HIPAA privacy and security obligations.\textsuperscript{71}

b. Liability and Enforcement Considerations

HIT-EHR related privacy and security concerns are further compounded by uncertainty surrounding liability for breaches in these areas. HIPAA limits its scope to covered entities and protected health information.\textsuperscript{72} Health plans, healthcare clearinghouses, and healthcare providers that transmit health information electronically are obligated to maintain the confidentiality of

\textsuperscript{67} Id. at 24.
\textsuperscript{68} Yaffee, supra note 22, at 340.
\textsuperscript{69} Maureen Young, Recent Federal Initiatives In Privacy And Information Security, PLI Order No. 19129, 509 (2009). Business associates are businesses that perform certain services for covered entities that involve the use or disclosure of protected health information. Jeffrey Taft, Privacy And Data Security In Service Provider Arrangements: Recent Developments, PRACTISING LAW INSTITUTE: PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROPERTY COURSE HANDBOOK SERIES. PLI ORDER NO. 14648 (2008).
\textsuperscript{70} Young, supra note 69, at 510.
\textsuperscript{71} Id.
\textsuperscript{72} Christiansen, supra note 18, at 22.
individually identifiable health information. While coverage also extends to business associates, HIPAA fails to regulate subcontractors and numerous individuals and organizations that handle protected health information because their activities fall outside these business processes. Examples of non-regulated activities and entities include provision of online health information services to customers, certain types of insurance carriers, researchers, employers, and marketing firms.

Additionally, HIPAA privacy and security regulations are further weakened by limited enforcement mechanisms. No individual remedies for redress are available to victims of HIPAA violations. HHS, which is charged with enforcement of HIPAA regulations, has no power to impose civil or criminal penalties against business associates of covered entities and no jurisdiction over subcontractors. While covered entities may liable for acts of its vendors, HIPAA defers to broader and more stringent state laws to close gaps in enforcement. Such an approach, however, causes greater confusion in liability determinations due to the variability in state laws. The weaknesses of these liability and enforcement provisions have been strengthened to some degree by ARRA, which subjects both covered entities and business associates to scaled civil penalties for violations arising from “willful neglect, noncompliance due to reasonable cause not involving willful neglect, and failure to properly correct violations.”

73 42 U.S.C. § 1320(d) to (d)-8 (2000).
74 Kenneth M. Rashbaum, *Offshore Outsourcing of Health Data Services*, 16 No. 6 HEALTH LAW. 24, 25 (2004); Dunlop, supra note 19, at ¶16.
75 Dunlop, supra note 19, at ¶16.
76 Christiansen, supra note 18, at 23.
77 Dunlop, supra note 19, at ¶16; Rashbaum, supra note 74, at 25.
78 Rashbaum, supra note 74, at 25.
79 Id.
80 Young, supra note 69, at 511.
2. (Illegitimate) Fears of Exposure to Privacy and Security Breaches Arising from HIT-EHR Implementation.

While the above overview of the current U.S. legal landscape confirms the need for further legislative reform, it is doubtful whether HIT-EHR adoption makes privacy and security breaches more prevalent or easier to commit. These fears abound in several manifestations: misuse of personal health information by offshore contractors assisting in IT operations;\(^{82}\) medical identity theft made easier for opportunist healthcare staff because of greater availability and circulation of data resulting from EHR accessibility;\(^{83}\) or hacking into health data repositories.\(^{84}\) With the exception of hacking, these types of thefts largely arise from human negligence and weakness – failings that will occur in any security system, and not because of unique HIT deficiencies.\(^{85}\) Just as significantly, evidence suggests that more security breaches occur with the use of more traditional record-keeping mediums than EMR/EHR formats. A 2011 review of HHS’s online publication of HIPAA security violations dating back to 2009 reveals that the majority (more than 60%) of breaches result from physical theft or loss of paper records and portable devices while only a minority implicate on-premise EMR server systems.\(^{86}\) If anything, EMRs/EHRs are arguably more secure than paper records when appropriate privacy and security mechanisms are in place.\(^{87}\) Unlike paper records, EMRs have monitoring and screening capabilities that include: record-keeping of who had access and what portions of a

\(^{82}\) E.g., Rashbaum, supra note 74, at 24.

\(^{83}\) E.g., Diagnosis: Identity Theft, BLOOMBERG BUSINESSWEEK, Jan. 8, 2007, http://www.businessweek.com/magazine/content/07_02/b4016041.htm.


\(^{85}\) See Barrow & Clayton, supra note 27, at 147.


\(^{87}\) Barrow & Clayton, supra note 27, at 146.
patient’s records were accessed; restricting certain users to certain types of information; and utilizing encryption to prevent document alteration or substitutions.88 Furthermore, the use of off-site storage technologies such as cloud-based EHRs offer another layer of security by keeping data on a host software company’s server and enabling access to such data via a web browser.89 This eliminates theft of data through hacked, stolen, or lost on-premise devices or systems.90 Moreover, cloud-based applications have a proven track record of protecting sensitive information, as other data-sensitive industries have long utilized such technologies.91

Because there is very little basis for dismissing HIT-EHR due to privacy and security concerns, it behooves the public and healthcare community to reconsider why it harbors such fears - especially when compared to other industries with similar concerns that have successfully capitalized on IT’s capabilities.92 The U.S. finance industry is an instructive example, as it regularly stores and transfers personal financial information across state and national borders in electronic form.93 For instance, banks routinely offer the convenience of round-the-clock services such as the use of automated teller machines, direct deposit of paychecks, personal computer banking, and electronic check conversion.94 When properly implemented, privacy and security safeguards for these types of financial transactions achieve conquerable effectiveness as those designed for HIT-EHR activities.95

---

88 Id.
90 Koploy, supra note 86.
91 Haughton, supra note 89.
92 Gantz, supra note 35.
93 Barrow & Clayton, supra note 27, at 147.
95 Gantz, supra note 35; Barrow & Clayton, supra note 27, at 147.
Just as significantly, the questionable bias against HIT-EHR is brought into greater relief in light of the similar legal challenges faced by the healthcare and finance industries. The finance industry suffers from a legal and regulatory regime that is arguably as, if not more, complex and confusing than those found in healthcare when privacy and security safeguards are implicated. Just as with personal health information, personal financial information is regulated at both federal and state levels. At the federal level, the Gramm-Leach-Bliley Act (GLBA) regulates sharing of personal financial information by financial institutions with third parties and affiliates. Critics of GLBA maintain that it is ineffective against theft because it not only shares similar inadequacies found in HIPAA, but is weaker than HIPPA in several areas. Examples of shared deficiencies include legal uncertainty and greater compliance costs in deferring to stricter non-conflicting state laws and no provision of a private right of action for GLBA violations. Additionally, GLBA is weaker than HIPAA in its privacy standards by failing to extend its coverage to past transactions and customers and curtailing its scope to a smaller category of entities. Furthermore, GLBA does not cover personal financial information shared with affiliates; this permits banks that have merged with other entities to divulge such data to these entities. Despite the confusion and inadequacies of these legal and regulatory frameworks, the finance sector has come to accept the need to meet or exceed industry “leading practice” and standards in order to remain competitive and maintain their reputations in

---

96 See generally, Bradley Macmahon, After Billions Spent To Comply With Hipaa And Glba Privacy Provisions, Why Is Identity Theft The Most Prevalent Crime In America? 49 VLLR 625 (2004); Taft, supra note 89.
99 See generally, Macmahon, supra note 96.
101 Rashbaum, supra note 74, at 28.
102 Macmahon, supra note 96, at 644-45.
103 Id. at 638, 641.
a business climate where consumers demand the conveniences and security afforded by industry IT processes.\textsuperscript{104} Once the benefits from widespread HIT-EHR adoption unfold, it is not implausible to expect that the healthcare sector will follow suit in incorporating costs of cross-border legal and regulatory compliance as a necessary business expense in order to operate profitably.

\textbf{III. THE WEAKNESSES OF CURRENT PRIVATE AND PUBLIC APPROACHES}

These challenges not only continue to delay the implementation of an HIT-EHR framework, but demand consideration of new approaches. Current private and public initiatives fail to resolve these challenges efficiently and effectively, as both primarily adopt a strategy of voluntary semantic interoperability to encourage IT adoption and communication among disparate systems. Unlike the use of uniform communication protocols in technically interoperable systems, semantic interoperability requires interfaces between disparate systems to ensure that information is unaltered in meaning when transferred and received.\textsuperscript{105} The analysis below argues for abandoning this semantic approach in favor of mandatory technical interoperability, as the latter would faster facilitate the national development of HIT-EHR with greater efficiency while concurrently helping to resolve some of the aforementioned legal considerations.


\textsuperscript{105} Baird, \textit{supra} note 16, at 233.
A. Inadequacies of Private Approaches towards National HIT-EHR Development

The U.S. private sector has initiated several strategies aimed at achieving semantic interoperability in HIT-EHR, none of which have resulted in widespread adoption. Several industry standard developing organizations have introduced mediating schema to facilitate communication among heterogeneous healthcare systems. A Continuity of Care Record (CCR) is one such initiative, which attempts to standardize electronic records through data extraction from existing EMR systems and utilize a common text export format enabling direct data transfer to the patient or a patient’s next healthcare provider. Developed in 2003, CCR was the result of grassroots efforts by healthcare providers and laypersons to establish an open and royalty-free standard to facilitate nationwide exchange of health information. Another similar, but incompatible standard is Clinical Document Architecture (CDA), which was developed by a nonprofit organization known as Health Level Seven International (HL7). This organization promotes CDA as the interface of choice for electronic health data exchange, and boasts “approximately 500 corporate members who represent more than 90% of the information systems vendors serving healthcare.” The incompatibility of these standards has led to the development of Continuity of Care Document (CCD), a harmonizing interface which blends CDA and CCR standards in order to bridge the gap between them by being compatible with both interfaces and other similarly formatted standards.

110 Id.
111 COREPOINT HEALTH, supra note 106, at 3, 5.
Despite such capabilities and in the case of CDA, command of such a large membership base among HIT vendors, most healthcare providers and vendors have refrained from adopting any of these interfaces.\(^\text{112}\) Widespread reluctance is attributed to the lack of a mandate requiring their use and the deterrent effect experienced by consumers because of the similarity and incompatibility of both standards.\(^\text{113}\) This low adoption rate indicates that dependence on the private sector is ineffective without proper guidance and coordination, as the resulting variations and differences in available solutions may only serve to reinforce existing gaps in interoperability.

Another private endeavor aimed at an EHR framework is the use of a Personal Health Record (PHR). The PHR is a database of a patient’s health information that is created and maintained by that patient.\(^\text{114}\) The patient herself is the gatekeeper to any part or all of her PHR to any interested party trusted by the patient.\(^\text{115}\) PHRs may be created online or on a patient’s own computer and may be freely provided by various entities, including: employers; healthcare providers;\(^\text{116}\) and large IT producers such as Microsoft and Google.\(^\text{117}\) Microsoft’s application, HealthVault, and Google Health both operate as an open source opt-in service for patients to customize their own health records.\(^\text{118}\) These applications, however, have yet to gain traction among an overwhelming majority of U.S. patients.\(^\text{119}\) A 2009 survey found that only 7% of U.S.

\(^{112}\) Id. at 3.

\(^{113}\) Id.

\(^{114}\) Terry & Francis, supra note 15, at 688.

\(^{115}\) Id.

\(^{116}\) Id.

\(^{117}\) WULSIN & DOUGHERTY, supra note 8, at 17.

\(^{118}\) Id.

patients have utilized PHRs.\textsuperscript{120} This adoption rate was higher than the preceding year,\textsuperscript{121} but such low adoption rates and the placement of responsibility on patients to maintain accurate and updated records should further behoove policymakers to consider alternative approaches that are far more efficient, reliable, and effective.

**B. Inadequacies of Public Approaches towards National HIT-EHR Development**

Similar to private initiatives, current public measures unsuccessfully utilize a voluntary semantic approach towards HIT-EHR interoperability. Federal efforts began in 2004, after the Bush Administration issued an Executive Order to implement nationwide HIT-EHR by 2014\textsuperscript{122} in response to mounting concerns over costs and quality of care related to paper-based medical records.\textsuperscript{123} The Executive Order appointed a National Coordinator for Health Information Technology to create and carry out the following policies and plans for HIT-EHR development: resolving privacy and security considerations, and facilitating interoperability, widespread adoption, and collaborative governance.\textsuperscript{124} The Obama Administration has continued this mandate by enacting the HITECH Act, which not only strengthened HIPAA regulations, as discussed above, but also provides significant funding to the Office of National Coordinator for Health Information Technology (ONC).\textsuperscript{125} Amounting to $19.2 billion, this budget supports the following initiatives geared towards voluntary semantic interoperability: Medicare and Medicaid reimbursement in exchange for “meaningful users” of HIT; regional and sub-national efforts towards health information exchange; and purchase of HIT systems and equipment and services

\textsuperscript{120} Id.
\textsuperscript{121} Id.
\textsuperscript{122} Dunlop, supra note 19, at ¶1.
\textsuperscript{123} WULSIN & DOUGHERTY, supra note 8, at 11.
\textsuperscript{124} Id.
\textsuperscript{125} Young, supra note 69, at 508.
for health IT for health centers.\textsuperscript{126} The ONC anticipates that these initiatives, in combination with other research and collaborative efforts with the healthcare sector, will lead to the development of interoperable standards for use in voluntary certification of HIT products and creation of EHRs for healthcare providers.\textsuperscript{127}

Rather than facilitating interoperability, such a strategy creates further fragmentation in the nation’s nascent and disconnected HIT landscape. While these aforementioned initiatives offer incentives for HIT implementation, the ONC’s failure to impose uniform technical standards or software as a starting point for the nationwide adoption process compounds the original dilemma of non-interoperability by increasing the number of disparate systems that are unable to communicate with one another.\textsuperscript{128} The below analysis of several of these initiatives demonstrates this assertion.

1. The Inefficiency and Ineffectiveness of “Meaningful Use” Criteria

The lack of specificity and guidance in the “meaningful use” criteria for Medicaid or Medicare reimbursement encourages the implementation of incompatible EMR systems and exposes healthcare providers to the costly risk of being denied reimbursement should they fail to meet these criteria.\textsuperscript{129} In order to receive incentive payments for EMR technology, healthcare providers must demonstrate use of certified EHR technology “in ways that can be measured significantly in quality and in quantity.”\textsuperscript{130} To achieve this goal, healthcare providers must

\textsuperscript{126} Id.
\textsuperscript{127} Id. at 508-09.
\textsuperscript{128} See Yaffee, supra note 22, at 347-48.
\textsuperscript{129} Yaffee, supra note 22, at 377-48, 352-353.
follow a graduated approach that requires compliance with specified objectives in three stages. Incentive payments are made over a four-year period, with each annual installment dispensed only after the healthcare provider proves it has successfully reached a certain transition level assigned to the year in question. This phased implementation-reimbursement approach seeks to bridge the gap between current technologies and healthcare provider IT experience with future technologies by revising and incorporating stricter objectives and measures over time. This fluid framework enables the ONC to modify and adopt new standards and criteria pertaining to EHR implementation and certification at each of the three meaningful use stages.

The inherent ambiguity of such a strategy has prompted stakeholders to urge for greater guidance and clarity, arguing that the HIT industry and healthcare providers would benefit from a more predictable and structured approach for standards adoption.

An analysis of meaningful use Stage 1, the first and only stage with identifiable objectives and measures and taking effect from 2010 to 2012, demonstrates how the ONC’s phased approach discourages interoperability and program participation. One primary weakness lies in the allowance of multiple technical and semantic standards as a first step towards EHR implementation -- an approach that encourages the use of disparate systems and increases the likelihood of reimbursement denial should the ONC eventually adopt a standard at a later stage.

---

132 Id. at 44459.
134 See Final Rule, supra note 133, at 1.
135 Id. at 15.
136 Id. at 15.
137 Final Rule, supra note 133, at 200-01.
that is different from one initially selected by a participating healthcare provider. For example, one objective requires meaningful use of patient summary records, which is the \textit{“capability to exchange key clinical information (for example, problem list, medication list, medication allergies, diagnostic test results), among providers of care and patient authorized entities electronically.”} The ONC has adopted CCR and CCD standards to fulfill this objective, but stakeholders protest that approval of more than one standard here would be “wasteful, counterproductive, confusing, time-consuming, and reduce interoperability.” These fears are valid when examining the capabilities of these standards. As noted earlier, CCD adopters may communicate with those using CCR but adopters of the latter standard lack the same harmonizing capacity.

These concerns are echoed in other Stage 1 objectives and adopted standards. For instance, the requirement for electronic prescribing mandates the use of HL7 messages or the NCPDP SCRIPT Standard when parties are part of the same legal entity but when parties from different entities are involved, only the NCPDP SCRIPT Standard or “other applicable adopted standards” are permissible. The imposition of different standards that hinge on party identity creates another layer of confusion and expense that may easily avoided by selecting one standard that accommodates all transaction scenarios from the outset. Another objective requires the recording of problem lists of current and active diagnoses in “structured data” and allows for the use of ICD-9 or SNOMED-CT® to provide that structure. Critics object that these standards serve different purposes, as ICD-9 carries out administrative and billing duties while SNOMED-

\textsuperscript{138} See Final Rule, \textit{supra} note 133, at 151; Yaffee, \textit{supra} note 22, at 347-48.
\textsuperscript{139} Final Rule, \textit{supra} note 133, at 149-50.
\textsuperscript{140} Final Rule, \textit{supra} note 133, at 39. CCR and CCD standards are discussed earlier in Part IV.
\textsuperscript{141} Final Rule, \textit{supra} note 133, at 151.
\textsuperscript{142} See Part IV.
\textsuperscript{143} Final Rule, \textit{supra} note 133, at 14.
\textsuperscript{144} Id. at 15.
CT® is designed to detail clinical descriptions of patient conditions – which means that if a healthcare provider adopts only the former standard, it will likely fail to meet the stated objective.145 While the ONC acknowledges this distinction, it shies away from offering stronger guidance by merely recommending the adoption of both standards.146 If anything, the ONC arguably excites greater uncertainty and inaction by noting that it “may eventually be able to adopt only one standard” after examining public input and experience related to both these standards.147

2. The Inefficiency and Ineffectiveness of Regional Health Information Organizations

The fragmentary effect of “meaningful use” certified EHR technology is unfortunately echoed in the ONC’s administration of its National Health Information Network (NHIN), a complimentary initiative aimed at fostering national standards for interoperability and privacy.148 Described as a “network of networks,” the NHIN seeks to foster the establishment and growth of Regional Health Information Organizations (RHIOs) to handle regional Health Information Exchanges (HIEs) as a means of furthering EHR implementation.149 RHIOs and HIEs may be used interchangeably, as they share similar structures and geographic scopes ranging from a local community to a multi-state region.150 An RHIO is “a neutral organization that adheres to a defined governance structure which is composed of and facilitates collaboration among the stakeholders in a given medical trading area, community, or region through secure electronic health information exchange to advance the effective and efficient delivery of healthcare for

---

145 Id. at 54-55.
146 See id. at 55.
147 Id.
148 See WULSIN & DOUGHERTY, supra note 8, at 11.
149 WULSIN & DOUGHERTY, supra note 8, at 11.
150 HIMSS TRANSFORMING HEALTHCARE THROUGH IT, DEFINITIONS AND ACRONYMS 1 (2009), http://www.himss.org/content/files/RHIO_Definitions_Acronyms.pdf.
individuals and communities.” Similarly, an HIE is “a project or initiative focused around electronic data exchange between two or more organizations or stakeholders” that employ common technology and standards to share information that may include clinical, administrative, or financial data. The analysis below will demonstrate that these initiatives contribute to the fragmentation of a national HIT-EHR framework by their limited geographic scope and adoption of different data exchange architectures among these initiatives, thereby hindering communication on a national level by fostering incompatible standards of communication.

RHIOS and HIEs are the building blocks for NHIN, which should be “a decentralized architecture built using the Internet, linked by uniform communications and a software framework of open standards and policies.” The ONC has acknowledged that a key challenge to meeting such a goal was the lack of “better-refined” standards. With regards to the development of HIEs, a 2006 study identified the establishment of 165 initiatives that have chosen to pursue different communication standards for interoperability. These selections include HL7, NCPDP, DICOM and X12. These standards are not only technically incompatible, but were also independently designed to serve different purposes and functions for different areas in the healthcare industry. Just as problematic are RHIOs, as their data architectures vary among organizations. A 2007 report estimates that 200 to 300 RHIOs are in

151 Id.
152 Id.
154 Id. at 2.
155 Id. at 5.
156 Id. at 5.
158 GOLDSTEIN & GROEN, supra note 153, at 5.
place, with each of these networks independently designed by various private healthcare IT vendors or relying on open source technology developed by the government. Furthermore, a 2009 joint Harvard-VA survey casts doubt on the ability of RHIOs and HIEs to effectively facilitate national data exchange, as only 13 of 247 initiatives examined in that study were able to meet the ONC’s Stage 1 meaningful use criteria while none likely possessed the technological infrastructure to conduct data exchange at the level required to realize the full benefits of an HIT-EHR framework.

3. The Inadequacy of Funding Initiatives

Additionally, the shortcomings of the above public initiatives are compounded by inadequate funding. Incentive programs, such as EHR certification reimbursement detailed above, fail to sufficiently cover the costs of HIT-EHR implementation and maintenance for many individual healthcare providers, small practices, critical-access and rural hospitals. For instance, EHR certification reimbursement compensates an eligible healthcare provider (e.g. physician) up to $44,000 through Medicare or $63,750 through Medicaid. Implementation costs alone ($30,000 or more) often exceed an individual healthcare provider’s annual net revenue ($100,000 to $200,000) after overhead costs are met. Additionally, the process of testing and certifying individual healthcare provider systems to ensure compliance with meaningful use criteria can range from $120,000 to $240,000. These costs, coupled with the requirement that an eligible healthcare provider absorb these expenses upfront, understandably

159 Id. at 9.
160 Id. at 5-6.
162 Yaffee, supra note 22, at 350-351.
163 42 CFR PARTS 412, 413, 422 ET AL., supra note 119, at 44451.
164 Yaffee, supra note 22, at 351.
165 Hillestad et al., supra note 38.
deter smaller scale healthcare entities with tight capital constraints from participating in HIT-EHR implementation.\textsuperscript{166}

RHIOS and HIEs likewise require greater funding reserves in order to remain operational, as public assistance only covers a substantial portion of start-up expenses.\textsuperscript{167} While this funding strategy may promote the RHIO/HIE establishment in communities with little interest in long-term support, the onus on stakeholders to financially sustain these initiatives results in the adverse effect of limiting data exchanges to those that provide a direct value to providers rather than facilitating the type of broader data exchanges intended by a national EHR infrastructure.\textsuperscript{168} Because these funding limitations discourage the participation of much-needed members in the healthcare sector, it behooves policymakers to reconsider the amount and allocation of such funds for a nascent and large scale endeavor as a national EHR framework.

**IV. A PROPOSAL FOR MANDATORY UNIFORM TECHNICAL STANDARDS**

The failure of existing private and public initiatives to overcome challenges to national HIT-EHR implementation demands consideration of new strategies. As the above analysis on both approaches demonstrates, reliance on voluntary participation by stakeholders and the private sector to come to consensus on standards for interoperability are inefficient and ineffective methods towards construction of a national EHR framework. While private market driven approaches towards interoperability have worked successfully in other industries, it is clear that there are stronger incentives for stakeholders in the healthcare sector to either forgo or independently pursue HIT implementation without consideration of harmonization. As discussed earlier, those who must shoulder the cost and responsibility of systems implementation

\textsuperscript{166} See Yaffee, \textit{supra} note 22, at 351.
\textsuperscript{167} Adler-Milstein, Bates & Jha, \textit{supra} note 161, at 670.
\textsuperscript{168} Adler-Milstein, Bates & Jha, \textit{supra} note 161, at 670.
and maintenance, primarily healthcare providers, enjoy no direct benefits for such an investment\textsuperscript{169} while HIT vendors stand to reap greater profits by creating customized systems that exclusively utilize their software and services.\textsuperscript{170}

With far reaching public policy goals of healthcare at optimal quality and cost at stake, a more centralized approach is required to shift incentives and eliminate competing interests in order to achieve widespread participation and streamline uniform standards for communication. In order to streamline this process in a more cost-effective and timely manner, this paper argues for a federal mandate requiring technical interoperability in systems implementation and updates to achieve an operational national EHR framework. To demonstrate the viability of this approach, this section will discuss the following: (1) feasible implementation models that may overcome the challenges of existing voluntary semantic strategies; and (2) successful precedence of such an approach in the U.S. and other countries, with a focus in particular on the federal legislation mandating the use of certain IT processes for the benefit of the U.S. finance industry.

A. Implementation of a Federal Mandate for Technical Interoperability

Federal legislation mandating technical interoperability is a feasible approach on constitutional and operational levels. The legal legitimacy of such a mandate may be based upon the U.S. Constitution’s Spending Clause, which has historically given Congress broad authority to spend for the general welfare as long as other Constitutional provisions are not violated.\textsuperscript{171}

\textsuperscript{169} \textsc{Wulsin & Dougherty}, supra note 8, at 9.
\textsuperscript{170} \textsc{Yaffee}, supra note 22, at 347-48.
\textsuperscript{171} See \textsc{Butler}, 297 U.S. at 66 (holding Congressional regulation of agricultural products through subsidies under the 1933 Agricultural Adjustment Act did not violate the Tenth Amendment as Congress has the constitutional power to tax and spend for the general welfare). Subsequent cases support the Court’s view of broad Congressional authority under the taxing and spending clauses. See \textsc{Steward Machine Co. v. Davis}, 301 U.S. 548 (1937) (Social Security Act establishing the federal unemployment system deemed constitutional); \textsc{Helvering v. Davis}, 301 U.S. 619 (1937) (Social Security Act’s old age pension program supported by federal taxes deemed constitutional); \textsc{Sabri v. United States}, 541 U.S. 600 (2004) (Federal criminal law banning bribery of state, local, and tribal officials of entities receiving at least ten thousand dollars in federal funds deemed constitutional).
The Spending Clause has been invoked to carry out federal mandates in healthcare regulation. These examples include the National Health Planning and Resources Development Act of 1974 requiring states to adopt certificate of need laws related to health facility planning\textsuperscript{172} and Medicare and Medicaid participation requirements, which impose operational standards and accreditation rules on healthcare providers in exchange for funding.\textsuperscript{173} Such precedence of federal mandates in the healthcare arena should enable the ONC to abandon its current voluntary Medicare-Medicare reimbursement model for “meaningful use” criteria adoption to require Medicare-Medicare participants to implement or update HIT systems in accordance with predetermined criteria in exchange for adequate compensation.

On an operational level, this federal mandate may be carried out in several ways, including compulsory use of a designated software product(s) by entities maintaining and transferring health data or the adoption of uniform technical standards, specifications, and infrastructure requirements for all HIT systems. By mandating particular software or protocols at the outset, the federal government and healthcare community would avoid the inefficiencies in time and costs of having to update or install new systems that the current scenario of multiple semantic and technical standards would eventually require. The nation’s severely underdeveloped HIT landscape also makes the use of such a mandate an optimal strategy as, discussed earlier, the vast majority of health data holders have yet to implement electronic data repositories. As a result, the need to update or replace any existing HIT systems that are incompatible with federal standards would be relatively far less costly and time consuming nationwide than the ONC’s current wait-and-see approach towards standard selection.

\textsuperscript{172} 42 U.S.C. § 300k, et seq. (1976).
\textsuperscript{173} See 42 USC §1395x(e) (2001) (hospitals); 42 USC §1395x(m) (home health services); 42 CFR §§484.1-484.55 (2001) (various types of providers).
Furthermore, the adoption of pre-determined criteria enables the ONC to provide funding for HIT implementation upfront rather than utilizing a staggered reimbursement model that is dependent on costly systems certification. By guaranteeing the funds at the outset, the ONC would go far in alleviating reluctance on the part of healthcare providers to invest in HIT systems discussed earlier in this paper.\footnote{174}

In addition to being a more cost-effective and time saving approach, a federal mandate for uniform technical standards is feasible because it can be built and expanded upon any one of several successful models already in operation on a smaller scale. For example, the VA’s “VistA” electronic record system discussed earlier, may serve as an ideal option as it not only has the capabilities to deliver healthcare at optimal costs and quality but is also one of the most prolific HIT-EHR systems in the world.\footnote{175} VistA software goes beyond supporting ambulatory and inpatient care in a variety of settings for over four million veterans nationwide to being utilized by The Department of Defense and many private U.S.-based and international healthcare entities.\footnote{176} Furthermore, VistA presents an economical solution when implementation costs are factored, as it is public domain software that is accessible to non-governmental entities.\footnote{177}

Another alternative to consider is the Indiana Health Information Exchange (IHIE) model, the longest running and one of the most viable RHIOs in the U.S.\footnote{178} Members in the IHIE network, which include 25 hospitals and over 5,000 physicians, utilize one messaging system to track, transfer, and maintain patient data.\footnote{179}
Finally, the adoption of uniform technical standards may help to alleviate some areas of legal ambiguity that currently plague federal and state privacy legislation pertaining to health data. For instance, federal selection of communications criteria may also include detailed security and privacy requirements that would reduce the ambiguity created by HIPAA’s failure to offer clarity on privacy and security protocols and having covered entities create safeguards tailored to their own organizations’ needs.

B. Government Regulation of IT Processes and Standards Have Been Successfully Employed in the U.S. and other Countries

A federal mandate for technical interoperability is not only feasible on legal and logistical levels, but is also supported by successful instances of government guidance over IT processes in various industries in the U.S. and abroad. In the U.S., for example, the finance industry has been able to operate more efficiently and profitably as a result of federal legislation requiring banks to accept and accommodate electronic imaging for expedited check collection processing. On an international scale, nations such as Australia have attained national EHR interoperability by appointing an agency to carry out centralized initiatives that include the establishment of uniform requirements for HIT systems. Furthermore, the European Union (EU) Commission’s adoption of GSM as the only permissible standard for the EU’s telecommunications market exemplifies the necessity of government intervention when private market forces fail to advance public policy goals. The below analysis will discuss each of these examples respectively to

180 See Christiansen, supra note 18, at 22.
181 Christiansen, supra note 18, at 23.
183 ARNOLD ET. AL., supra note 14, at 2.
184 Baird, supra note 16, at 270.
demonstrate that they share similar challenges and circumstances with the U.S. healthcare sector, thus providing further justification for the adoption of a similar solution for the latter.

1. Federal Legislation Mandating Acceptance of Electronic Check Imaging: Check Clearing for the 21st Century Act

Similar to the U.S. healthcare sector, the U.S. banking industry has globalized as a result of technological advances and consumer mobility enabling and requiring financial transactions and business operations to be performed on national and international levels. And similar to the current reluctance on the part of healthcare entities to invest in HIT because of high costs, greater exposure to privacy and security threats, and uncertain benefits, financial institutions were initially hesitant to adopt emerging technologies in the early stages of the industry’s global expansion for these reasons. One area of resistance lay with transforming the banks’ check clearing process from paper-based to electronic check imaging transfers, an application that both improved the efficiency of bank payment systems and met the changing needs and expectations of consumers. It was only after the federal government enacted the 2003 Check Clearing for the 21st Century Act (Check 21) requiring banks to accept electronic check imaging that such technology took hold in the industry and enabled banks and consumers to benefit from savings in cost and time.

---


188 CHECK 21, supra note 187, at 11; FEDERAL RESERVE SYSTEM’S PAYMENTS SYSTEM POLICY ADVISORY COMMITTEE, A SUMMARY OF THE ROUNDTABLE DISCUSSION ON RETAIL PAYMENTS FRAUD 11 (2007), http://www.federalreserve.gov/paymentsystems/retailpmtfraud/retailpmtfraud.pdf [hereinafter FEDERAL RESERVE PSPAC]. The Federal Reserve System’s Payments System Policy Advisory Committee has an ongoing program to discuss payments system developments and barriers to innovation with the payments industry and relevant payments
The challenges of changing market conditions in the past two decades and widespread disruption to the U.S. economy in the wake of September 11, 2001, prompted the federal government to enact Check 21 in the endeavor to encourage innovation and insulate the U.S. economy and consumers from the weaknesses of a paper-based check collection system.¹⁸⁹ Prior to Check 21’s passage in 2003, state laws governed bank deposits and collections in their jurisdictions and all states applied the Uniform Commercial Code (UCC) – with local variation in some instances - to govern the check clearing process.¹⁹⁰ The UCC requires the physical return of deposited checks to the issuing bank unless alternative arrangements are made between the involved banks in question.¹⁹¹ As the nature of retail transactions in the U.S. began to change as a result of technological advances and rising popularity of online purchases, this paper-based process proved ill-equipped to deal with the growing trend among consumers in using electronic payments.¹⁹² Additionally, it was common for delays to occur because of bad weather and transportation mishaps.¹⁹³ The tragedy of September 11, 2001, underscored such inefficiencies by delaying the clearances of checks worth nearly $50 billion for several days due to disruptions in air and ground transportation.¹⁹⁴

To encourage banks to better respond to these market changes and prevent processing delays, Check 21 overrides UCC requirements by permitting the use of electronic check imaging system participants. As part of this program, the committee hosted a roundtable discussion with industry leaders on issues involving fraud in retail payments. The roundtable discussion was held at the Federal Reserve Bank of Minneapolis on March 27, 2007.

¹⁹² CHECK 21, supra note 187, at 4.
¹⁹³ Barry, supra note 182, at 132.
¹⁹⁴ Id. at 131-32.
and check truncation absent an exchange agreement.\textsuperscript{195} While banks are not required to image checks, banks are allowed to utilize this application and recipient banks must accept transmission of electronic check images and substitute checks in place of original checks.\textsuperscript{196} Conversion from paper-based to electronic transfers benefit banks and consumers in several ways: (1) millions of dollars in transportation costs as banks no longer need to receive physical checks;\textsuperscript{197} (2) absence of delays due to weather or transportation issues make the check collections process faster and more efficient;\textsuperscript{198} (3) and greater availability of deposit-taking ATMS in more locations provides consumers with more choices and convenience.\textsuperscript{199} The realization of these benefits has led to a rapid increase in the use of imaging technology.\textsuperscript{200} In January 2007 alone, the Board of the Governors of the Federal Reserve System (Federal Reserve) reported an almost five-fold increase in the number of electronic image transfers.\textsuperscript{201} By fostering acceptance of technological innovations such as electronic check imaging, the federal government helped the banking industry embrace an application that has improved their business processes, raised profitability, and increased their consumer base.\textsuperscript{202}

Just as importantly, it is instructive to note that heightened security concerns over imaging technology were unfounded following industry adoption of this application.\textsuperscript{203} Just as with the healthcare industry, the banking industry had to wrestle with public concerns over privacy and security as a result of media scrutiny on financial data breaches, all of them

\begin{footnotesize}
\textsuperscript{195} S. REP. NO. 108-79.
\textsuperscript{196} Barry, supra note 182, at 130-31, 134.
\textsuperscript{197} Id. at 131.
\textsuperscript{198} Id. at 132
\textsuperscript{199} Id. at 138.
\textsuperscript{200} CHECK 21, supra note 187, at 11.
\textsuperscript{201} Id.
\textsuperscript{202} FEDERAL RESERVE PSPAC, supra note 188, at 11.
\textsuperscript{203} CHECK 21, supra note 187, at 1; FEDERAL RESERVE PSPAC, supra note 188, at 3.
\end{footnotesize}
instances which were unrelated to the imaging technology. In the case of electronic check imaging, both the banking industry and consumers were fearful that fraud may arise as a result of hacking into a bank’s database to retrieve unauthorized access to customers’ private financial information. Also worrisome was threat of financial losses resulting from double processing of a single check or errors in the check conversion process from paper to image. Such fears, however, were misplaced, on the part of both banks and consumers. A 2006 review of consumer complaints maintained by the Federal Reserve revealed few concerns with imaging technology. Banks reported that the electronic check imaging process actually reduced risk of fraud because faster check clearance enabled banks to (1) quickly obtain information that fraud is taking place and (2) return a fraudulent check before funds are made available to the depositor. While electronic imaging is clearly a different application than those utilized in HIT, this scenario is a relevant comparison because it further underscores the power and misperception of fear of new technologies discussed earlier in this paper.

1. Lessons in Interoperability from Abroad: Australia’s EHR Infrastructure and EU Adoption of One standard in the Telecommunications Industry.

In addition to the impact of federal Check 21 legislation and imaging technology in the U.S. banking industry, nation and nation-groups such as Australia and the EU offer insights into the benefits of government guidance to achieve HIT-EHR interoperability. In Australia, the Council of Australian Governments created a non-profit agency, the National E-Health

---

204 Federal Reserve PSPAC, supra note 188, at 4. In 2007, for example, media attention on the following financial data breaches have triggered these fears: T.J. Maxx Company compromised 45.7 million credit and debit card numbers of its customers; Dai Nippon printing company was victim to theft of 9 million pieces of customer information; Stop and Shop Supermarket Company experienced theft of an unknown number of customers’ credit and debit card information. Id.
205 Barry, supra note 182, at 138.
206 Id. at 134.
207 Federal Reserve PSPAC, supra note 188, at 3.
208 Id.
Transition Authority (NEHTA), to advance a centralized approach towards HIT-EHR interoperability. Prior to deployment of this strategy in 2004, Australia struggled with national EHR implementation in large part because of the plethora of small and independent HIT systems already in existence that failed to be interoperable or scalable. To ensure uniformity nationwide, NEHTA is charged with setting standards and other infrastructural protocols for adoption by eHealth systems of all levels of government. Examples of common standards and protocols for shared use include: (1) nomenclature and messaging standards; (2) national directories of relevant terms and names; (3) and unique personal and healthcare provider identifiers. In particular, NEHTA’s initiatives quieted the concerns of Australia’s healthcare community because prior to its existence, “there was no single approach to developing e health [sic] components.” By determining such criteria at the outset, a 2007 review of NEHTA’s progress concluded that it had established a strong foundation for broad-based EHR implementation on a national level.

While Australia’s examples underscores the power of central direction over diverse and uncoordinated private efforts in reaching HIT interoperability, the EU’s imposition of one technical standard in its telecommunications industry highlights the importance of protecting public policy goals when the private market fails to do so. The EU’s adoption of GSM standard for the European cellular network reflects not only its mission to promote a common market

---

209 ARNOLD ET. AL., supra note 14, at 2.
210 RHONDA JOLLY, THE E HEALTH REVOLUTION – EASIER SAID THAN DONE 24 (2004), http://www.aph.gov.au/library/pubs/rp/2011-12/12rp03.pdf. It should be noted that subsequent evaluation of Australia’s centralized approach has stalled and encountered stakeholder dissatisfaction because of the following issues, which are unrelated to a centralized approach towards standards determination: privacy, access to records, funding, and questions of competency. Id. at 26, 50.
211 ARNOLD ET. AL., supra note 14, at 4.
212 Id.
213 JOLLY, supra note 210, at 24.
214 Id.; ARNOLD ET. AL., supra note 14, at 4.
among its member states but also its goal of consumer protection.\textsuperscript{215} Prior to such a mandate, national monopolies dominated the EU telecommunications market and created different technical standards that were incompatible from one member state to the next.\textsuperscript{216} Consumers suffered from high costs and inconvenience as a result, as cell service failed to work across borders and consumers were forced to buy several phones while traveling among member states.\textsuperscript{217} The EU mandate for one technical standard, GSM, enabled cellular phone portability across the EU by removing these challenges.\textsuperscript{218} Just as with the detrimental impact of incompatible technical standards on consumers in the EU, the plethora of competing and incompatible HIT systems in the US prevent the fruition of critical public goals of health services at optimal quality and costs. As a result, U.S. policymakers should reconsider its current strategy of prolonged private market reliance on a variety of incompatible technical standards and interfaces and focus instead on unilaterally selecting proven common criteria to propel the nation towards HIT-EHR interoperability.

VI. CONCLUSION

While the US lags behind many other countries in the construction of a national EHR infrastructure, it does not follow that its path towards HIT-EHR implementation and interoperability should be as plodding or inefficient. As this paper has demonstrated, current initiatives hinder or prevent these goals by encouraging the growth of incompatible technical and semantic standards through reliance on voluntary, private-market driven strategies. While such traditional decentralized approaches may appease U.S. policymakers and constituents who prefer

\textsuperscript{215} Baird, \textit{supra} note 16, at 269, 271.
\textsuperscript{216} \textit{Id.} at 270.
\textsuperscript{217} \textit{Id.} at 271.
\textsuperscript{218} \textit{Id.} at 270.
status quo solutions, they are inadequate to the task of resolving the competing interests of stakeholders in the healthcare community as well as widespread concerns over breaches in health data privacy, security, and liability. Fortunately, the experiences of other industries and nations facing similar challenges and circumstances offer instructive insights by pointing to more revolutionary approaches in order to maximize the benefits of technological innovations and achieve public policy goals. The U.S. finance industry, in particular, faced several crises that forced it to embrace nontraditional solutions. As discussed earlier, federal legislation was enacted to facilitate industry-wide adoption of electronic check imaging in the check collections process in the wake of September 11, 2000 – a tragedy that crystallized the inefficiencies of paper-based check transfer by halting all air and ground transportation. Similarly, the Year 2000 Problem (otherwise known as Y2K or Millennium bug), compelled the financial industry to adopt new business strategies, such as outsourcing work abroad or sponsoring foreign programmers, in a bid to prevent computer failures when clocks rolled over into 2000. In doing so, financial entities had to abandon longstanding industry-wide prejudices against such practices, which were based upon perceived violations of corporate policies or breaches of customer data privacy. These crises forced the finance industry to become more flexible in adopting nontraditional and more cost-effective solutions to address new challenges within a limited timeframe. As we face a similar dilemma in healthcare marked by escalating costs and growing discontent, U.S. policymakers and the public must acknowledge the necessity of adopting revolutionary approaches in the healthcare industry, as challenges to the feasibility of


220 Id.

221 Id.
such strategies are mainly rooted in unfounded fears and misperceptions of new technologies and processes.