The Evolving Regulatory Framework for Health Information Technology in the U.S.

Completed Research Paper

Ravi Behara
Florida Atlantic University
rbehara@fau.edu

C. Derrick Huang
Florida Atlantic University
dhuang@fau.edu

Jahyun Goo
Florida Atlantic University
jgoo@fau.edu

Abstract

With a large potential impact and a high level of complexity in the deployment of IT in healthcare in the U.S., the role of the federal government in setting the context is important. This study provides an overview of the current and evolving regulatory environment that healthcare organizations in the U.S. face when they deploy essential information technologies. We establish the framework of analysis using the socio-technical perspective of the systems theory and analyze the five key areas of healthcare IT regulations: electronic health records, clinical decision making, healthcare information exchange, privacy and security, and mobile and electronic health. We conclude by providing overview remarks on the overall structure of the HIT regulations in the U.S.

Keywords

Healthcare information technology, electronic health records, regulation, health information exchange, mobile health, privacy, security

Introduction

The discovery, development, and use of advanced medical technologies to provide high-quality care have always been a hallmark of the U.S. healthcare leadership in the world. Such technologies include advanced clinical solutions driven by the latest pharmaceutical- (biochemical) and biotechnology- (genetic, biologic) based treatments, advanced medical diagnostic equipment and instrumentation, and medical device technologies for individual patients. But the cost of providing healthcare is also increasing at an alarming rate. The U.S. healthcare spending in April 2012 was at a seasonally adjusted annual rate (SAAR) of $2.79 trillion, which represents nearly 18 percent of GDP (Altarum, 2012). The healthcare costs are increasing for many reasons, including a greater use of expensive and innovative methods of care, demographic changes with a larger number of elderly needing services, higher insurance costs due to increasing litigation against service providers, and an inefficient delivery system. The size and rate of growth of this cost became a major national concern, and information technology (IT) can potentially address many of the root causes.

The development and deployment of IT to facilitate efficient and effective care delivery have been conspicuously slow in the U.S. healthcare industry. This is perhaps because the U.S. healthcare system not only has to deliver care to a larger population, it must do so in a more complex and a combined public/private sector context. Some advanced economies with smaller populations and national healthcare systems have pioneered the use of information technology ahead of the U.S. With such a large potential impact and a high level of complexity in the deployment of IT in healthcare, the role of the federal government in setting the context is important. This study aims to provide an overview of the
The evolving regulatory environment that healthcare organizations in the U.S. face when they deploy essential information technologies.

This paper begins with a socio-technical systems based framework to better understand the environment of healthcare regulations. We then provide a brief overview of the regulatory origin for the current push toward wide-scale Electronic Health Records (EHRs) adoption across the United States as the basis for the development of healthcare IT regulations. We proceed to discuss the continued evolution of the regulatory framework for the five key elements of healthcare IT and conclude by providing some overview remarks on the overall structure of the HIT regulations in the U.S.

**Healthcare Service: A Socio-Technical Systems Perspective**

A systems approach provides healthcare service regulators and researchers with appropriate frameworks in which to develop regulations and studies related to healthcare IT. Checkland (1981) identifies four types of systems based on an intuitive attempt to describe the external world: natural systems, physical designed systems, designed abstract systems, and human activity systems. Human activity systems encompass all types of human activities such as governments and organizations. Such systems perpetuate their own existence through a number of important functions: adaptation, regulation, renewal, communication, and transformation. Four broad categories of systems perspectives—Living Systems Theory, Socio-Technical Systems, Systems Dynamics, and Non-linear Systems Paradigm—are commonly associated with the study of human activity systems; among them the Socio-Technical Systems is most related to HIT regulations.

Systems theory provides appropriate integrative models with which to understand service organizations and the change initiatives they are implementing. The Socio-Technical Systems (STS) perspective was developed to explain the critical relationships that exist between people and technology. The STS approach is a guide to ensure that the social system and its individual members are an integral part of the organizational improvement efforts in order to facilitate a smooth transition of people and technology to a new state. The STS concept is simple: It states that a change in structure and technology must necessarily consider the impact on human efforts. The difficulty is that reactions of personal frustration and tensions could surface at unexpected parts of the social system. Therefore, STS calls for a joint-optimization of the social and technical subsystems in an organization (Emery, 1959). Joint-optimization “regards man as complementary to the machine and values his unique capabilities for appreciative and valuating judgment. He is a resource to be developed for his own sake” (Trist, 1981, p. 42). In such a joint-optimization approach, the most effective arrangement of human organizations is one that integrates the demand of both technical and social aspects of interactions. In the case of healthcare, as the complexity in organizations, delivery structure, and the overall economy continues to increase, simplistic analyses of interactions that exclude technical or social systems cannot provide answers for improvement. In considering the impact of information technology on healthcare, an STS approach, shown in Figure 1, provides a valid alternative framework for analysis.
The obvious element of the STS framework for healthcare IT is the technology component that makes for improved operational efficiency and effectiveness, measured by the better quality, safety, and reduced cost of the service. But, as technology adoption crosses a threshold, it allows for the possibility of innovative business models to emerge. These service innovations are also being introduced in small pockets, with the intent that multiple successful efforts will eventually reach a tipping point and lead to broad-based adoption. At the crossroads of healthcare IT and service innovation adoption emerges the core objective of patient-centered care, which gives meaning to all activities in healthcare. At the same time, both technology and service innovation in healthcare appear to follow an approach of incentive-based adoption that is being pushed toward a broad-enough acceptance so as to become the “new normal.”

But none of these work in a vacuum. An essential regulatory environment for the deployment of various IT initiatives in healthcare services situates and coordinates the technology, innovations, and financial incentive to deliver patient-centered care. In such a view, HIT implementation is not only about EHRs or any other technologies. An implementation of a true “system of technologies” is under way. We can see that in addition to the typical transactional hardware and software systems in EHRs, there is a significant communication element in the deployment of health information exchanges, cloud-based services, and mobile applications. In addition, the use of decision support tools, an often-ignored core of technology, is gaining its rightful place at the center of the IT deployment effort. But in the interaction of such a socio-technology system, long-term success of technological initiatives is based on sound standards, both technical and regulatory. In the case of healthcare, due to the larger public good involved, the need for a coherent regulatory environment is particularly important.

**Regulatory Drivers**

The American Recovery and Reinvestment Act of 2009 (ARRA) became law in February 2009 as a significant effort to jumpstart a stalled U.S. economy. A key objective of ARRA was to modernize the nation’s infrastructure, and promoting and expanding the adoption of health information technology (HIT) are among the primary means to achieve that goal. This was addressed by the Health Information
Technology for Economic and Clinical Health Act (HITECH Act), enacted under Title XIII of ARRA. It authorizes the Centers for Medicare and Medicaid Services (CMS) to provide a reimbursement incentive for physicians and hospital providers for the “meaningful use” of “certified” EHR technology (Blumenthal, 2009). This reimbursement, together with other related investments, totals more than $17 billion for HIT-related expenditures within ARRA (AthenaHealth, 2009). Such a financial incentive is significant, as it represents the biggest federal technology initiative since the Manhattan Project for the creation of the atomic bomb during the Second World War (Blumenthal, 2009). At a time when the cost escalation of healthcare and the aging demographic profile of the U.S. are seemingly crippling the healthcare systems and impacting competitiveness of the country, this HIT initiative is regarded timely, critical, and strategic (Hillestad et al., 2005). But in many ways, this technology initiative can be far more difficult than the Manhattan Project, as it attempts to address a “distributed problem” with individual physician practices, hospitals, and other service providers all having to make a transition to integrated and secure EHR systems. In addition, the HITECH Act also provided the Department of Health and Human Services with the authority to disseminate regulations and guidance to support the development of an interoperable, private, and secure nationwide health information technology infrastructure through the newly formed Office of the National Coordinator for Health Information Technology. This has unleashed a major IT overhaul of the entire healthcare sector in the United States, and the Health Information Exchange (HIE) infrastructure has started to emerge as the central nerve system of regional or national HIT.

The EHR implementation initiative is a combination of initial incentives for adoption and future penalties for non-adopters. Incentive payments began in 2011 and will gradually phase out in 2016 for Medicare EHR, while Medicaid EHR incentive payments end in 2021. Starting in 2015, providers are expected to have adopted and be actively using an EHR in compliance with the “meaningful use” definition, or they will be subject to financial penalties under Medicare (and later under Medicaid) reimbursement rules.

The incentives paid under the HITECH Act paints a picture of the scope of EHR implementation to date. The EHR incentive program reported that starting in 2011 and as of March 2012, $4.48 billion was paid out in incentives. This included over $792 million to 44,014 Medicare-eligible professionals, over $628 million to 29,931 Medicaid-eligible professionals (physicians, dentists, nurse practitioners, etc.), and $3.06 billion to 2,667 eligible hospitals that serve both Medicare and Medicaid recipients (CMS, 2014a). While such payments are commonly regarded as a “government program,” it must be recognized that the CMS is in fact a customer of the private for-profit and not-for-profit physician practices and hospitals and the largest payer to the healthcare service providers. In effect, what happened can be seen as a large, concerned, and motivated customer motivating the service providers to improve their service delivery by paying for their use of technology. The rationale of such an incentive is the customer’s (CMS) belief that EHR technology implementation will result in improved quality, better safety, and ultimately, a lower cost of healthcare service. Eventually, it is hoped that this positive impact will spread to customers of other for-profit payers (insurance companies), thereby improving healthcare service to all citizens in the U.S.

Beyond the individual use of EHRs, the need to coordinate patient care across varied providers has resulted in the development of HIEs (Fontaine et al., 2010). Most HIEs are formed to share general patient and other care information among healthcare providers and organizations within a specific geographic area. However, others are designed for unique purposes, such as to collect information about participants involved in a state Medicaid program. There is no single source of the formation of HIEs; they are being established by state governments, private organizations, public-private partnerships, or collaborations among providers (ECRI Institute, 2012). The complexity of the structure and administration of HIEs effectively creates a sophisticated network that handles the supply chain of patient information in healthcare today to facilitate coordination as a way to improve quality, safety, and efficiency of patient care.

When examining such large-scale, complex regulatory mandates with financial incentives and penalties that drive the implementation of healthcare information technologies, one has to recognize that this is not simply a one-shot build-out of the healthcare service infrastructure to improve quality, safety, and cost. Instead, the regulatory environment is constantly changing and evolving to meet current needs and accommodate emerging technologies and patient requirements. In the next sections, we attempt to examine the themes of current regulatory framework for HIT in the U.S.
Healthcare IT Regulatory Environment

Surveying the current landscape of key information technologies and systems being deployed in healthcare, we identify five main areas as the focus for examining the current regulatory structure of HIT in the United States:

- EHR Adoption
- Clinical decision support
- Interoperability and HIE implementation
- Healthcare information privacy and security
- Mobile and electronic health

EHR Adoption

EHR adoption is the cornerstone of the HIT initiatives. As mentioned earlier, EHR implementation has been primarily driven by federal financial incentives and potential penalties. These incentives are closely tied to the notion of “meaningful use” (Blumenthal and Tavenner, 2010; Halamka, 2010; Markle Foundation, 2009), which is the specific targets, defined by CMS, that must be attained so that the healthcare providers can be eligible to receive incentive payments. As it currently stands, providers have to implement EHR systems that are certified by CMS, and the outcomes of such deployments would be evaluated in three stages of meaningful use (MU). The three stages have distinctive focuses: Stage 1 targets data capture and sharing; Stage 2 centers on advanced clinical processes; and Stage 3 focuses on improved outcomes (CMS, 2013). Currently, only MU Stage 1 is fully defined for providers to accomplish. Some of the main elements of MU Stage 1 are for providers (professionals and hospitals) to use Computerized Physician Order Entry (CPOE), to generate and transmit permissible prescriptions electronically (eRx), to incorporate clinical lab test results into certified EHR technology as structured data, to record and chart changes in vital signs, maintain active medication, allergy, and diagnoses list, to provide patients with an electronic copy of their health information, to perform medication reconciliation at relevant encounters and each transition of care, and to send reminders to patients per patient preference for preventive/follow-up care. The objective of Stage 1 meaningful use is clearly targeted at ensuring better coordination of care among providers, reduced errors, and improved involvement of the patient through information. Stage 2 MUs, however, are targeting the next level of outcomes, such as incorporating clinical lab-test results, using clinically relevant information to identify patients for receiving follow-ups, and using clinical decision support to improve performance. Currently, Stage 3 MUs are yet to be defined. Stage 2 MUs implementation is already under significant dispute and delay, and Stage 3 MUs is not scheduled to begin until 2017 (CMS, 2014b).

In addition to CMS, other government bodies are involved in the implementation of EHR. The Agency for Healthcare Quality and Research (AHRQ) conducted a study that looked into the need to promote standards in usability and information design in the development of EHRs (Armijo et al., 2009). The National Institute for Standards and Technology (NIST) is involved in setting technical standards for HER, such as the guidelines for technology vendors and users to evaluate the usability of EHR (NIST, 2008) and recommendations for integrating EHR into clinical flow in hosting organizations (NIST, 2014).

Studies analyzing the impacts and outcomes of EHR implementation with the Meaningful Use mandate to date have reported mixed results. Buntin et al. (2011) conducted a comprehensive analysis of 154 peer-reviewed studies over a three-year period and found largely positive effects of health IT on care delivery and on provider and patient satisfaction. Specifically, they found that over 92 percent of the studies reached positive conclusions on the effects of the health IT implementation, and that these positive effects were present in both large healthcare systems as well as smaller practices. But they also found studies reporting shortcomings and highlighting the importance of the “human elements” such as strong leadership and staff support for the change when transitioning to health IT. At the other end of the spectrum, there are significant concerns about the systems implementation and the outcomes (Hogan and Kissam, 2010; Jones et al., 2011). And since usability and information design are highly correlated with successful implementation and effective use of computer systems, these disciplines should be promoted in the EHR market to ensure realization of the benefits expected from federal investments in HIT. Even deeper are the concerns that not all EHRs have the same design effectiveness across multiple clinical disciplines. Consultants from Booz Allen Hamilton found in a study that there are deep-rooted problems
in the technical design of EHRs beyond usability (Leslie, Doscher, & Toner, 2012). For instance, EHRs were originally designed for billing, coding, and documentation, so their developers had few incentives to maximize quality and efficiency; such an initial focus turns out to be a major roadblock to EHR innovation. And there is a limited focus on information exchange since the majority of EHRs operate on closed networks that do not easily connect with other systems. This limits its usefulness in care coordination and delivery.

While it is still being debated whether the federal government or the private sector should spur EHR adoption and innovation, four themes have emerged on the future of EHRs in the next few years (Leslie et al., 2012):

- Further integration with mobile technologies
- Greater affordability and personalization for providers
- More accessibility and interoperability with other systems
- Greater emphasis on patient centeredness to encourage patient engagement in care decisions and communication with providers

Another key concern is the growing shift to cloud-based EHRs (Hirsch, 2012). This Software as a Service (SaaS) approach appears to have many advantages—EHR response time (such as the loading time between clicks), customer support (such as frequent updating and enhancements), product quality/usability, and “bang for the buck”—to the healthcare organizations. Although cloud-based solutions may potentially induce concerns such as access to and ownership of patient data, no specific regulatory governance principles have been established.

Thus from a regulatory perspective, while there is a growing adoption of existing EHRs with positive outcomes via the use of incentives and penalties, there are also many deep-rooted technical and design issues that remain to be addressed. Some of these are being addressed through the use of new and emerging technologies, while others must be based on a fundamental rethinking of the way the EHR solutions are developed. There continues to be both optimism and opportunity to improve, making this space a dynamic area of continued development in HIT.

**Clinical Decision Support**

The Healthcare Information and Management Systems Society (HIMSS), the professional society for HIT professionals, defines clinical decision support as a process for enhancing health-related decisions and actions with pertinent, organized clinical knowledge, and patient information to improve health and healthcare delivery (HIMSS, 2012). Information delivered can include general clinical knowledge and guidance, intelligently processed patient data, or a mixture of both; information delivery formats can be drawn from a rich palette of options that includes data and order entry facilitators, filtered data displays, reference information, alerts, and others. Clinical decision support has been recognized to provide significant patient care benefits; it is a highlight of the EHR system implementation as a logical extension of the increased data collection that is integral to the widespread use of EHR technologies (Kauscher et al., 2003; Kuperman et al., 2007). Despite its potential for improved patient safety and clinical outcome, clinical decision support efforts are still in their early stages, and the regulatory framework is not yet formed, except its inclusion in the Meaningful Use program. To date, its implementation has not been secured: Although clinical decision support was initially expected to be first implemented in Stage 2 and extensively in Stage 3, specific core requirements have yet to be established.

**HIE Implementation**

There have been many efforts in the past few decades to share healthcare information among service providers. For various reasons, despite heavy promotions, Health Information Exchange implementation did not reach the threshold of success. The HITECH Act allocated $2 billion to support HIE activities and created the Office of the National Coordinator for Health IT (ONCHIT) to direct the build-out effort. In particular, two main HIE initiatives are supported. The first is a $560 million effort at the state level, with the State Health Information Exchange Cooperative Agreement Program to facilitate and expand the secure electronic movement and use of health information among organizations within/between states in accordance with nationally recognized standards. The second $200 million
initiative is a smaller, targeted community program to further enhance ongoing HIE efforts by organizations and agencies. The widespread integration with HIEs is slated for Stage 3 MU of EHR.

Some initial results of HIEs are encouraging. For instance, Frisse et al. (2012) found that the sharing of electronic data among 12 Memphis-area emergency departments reduced hospital admissions and redundant imaging tests. The total annual savings of $1.9 million were largely attributable to avoidance of admissions. At a wider state level, the Washington State Healthcare Authority started using an HIE in June 2012 to share patient information among its emergency departments and physicians, thereby reducing unnecessary emergency room visits. As a result, a savings of $31 million was expected (Bowman, 2012).

The long-term goal for HIE efforts is the development of a broad-based interoperability and a national network, as represented by the Nationwide Health Information Infrastructure (NwHIN) under ONCHIT. The NwHIN incorporates a community of providers to create the standards and services that, within a policy framework, enable simple, directed, routed, scalable transport of information over the Internet to be used for secure and meaningful exchange among known participants in support of meaningful use. Such healthcare service platforms are the early markers of policies and standards that link individual systems (EHRs) with regional cooperatives (HIEs). A key prerequisite for such initiatives to be successful, however, is the assurance of privacy and security of healthcare information, both within EHRs and in interoperable HIEs, as discussed in the next section.

Healthcare Information Privacy and Security

The privacy and security of healthcare information is governed by the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules and enforced by the Health and Human Services (HHS) Office for Civil Rights (OCR) at the federal level. The HIPAA Privacy Rule applies to all forms of patient health information (PHI), be it electronic, oral, and paper. It provides federal protections for personal health information held by all covered entities including healthcare providers, health plans, and healthcare information clearinghouses. The HIPAA Privacy Rule gives patients an array of rights with respect to that information and at the same time permits the disclosure of PHI needed for patient care and other important purposes with the consent of patients. At the intersection of HIT, the HIPAA Security Rule applies to electronic patient health information (EPHI) and specifies a series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of patients’ electronic protected health information.

As required by Section 13402(e)(4) of the HITECH Act, breaches of unsecured protected health information affecting 500 or more individuals must be reported to the HHS, to be posted at [www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html](http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html). A quick review of this website shows that there the number of breaches have steadily gone up since the beginning of public records, with 49 breaches reported in 2009 (September through December), 206 in 2010, 208 in 2011, 213 in 2012, and 223 in 2013. These breaches involve anywhere from a few hundred individual medical records to hundreds of thousands or even millions of records being compromised in a single event. A total of more than 20 million individuals were affected by these security breaches. The breached data storage includes paper, laptop, removable storage drives, and network servers, and the methods of attacks are not all technology-oriented. In fact, there is a significant level of internal (employee) attacks, and many of the other breaches are simply the result of misplaced laptop or removable hard drives. The common thread underlying all these breaches was a lack of security planning and protocols, and, hence, there is a growing realization that protecting security and privacy is an ongoing managerial responsibility. Accordingly, National Institute of Standards and Technology published guidelines for implementing HIPAA security rules (NIST, 2008), although it has no enforcement authority.

Unlike the EHR and HIE initiatives, no specific financial incentives (under ARRA or any other legislations) exist to implement HIPAA privacy and security rules in the context of EPHI. The incentives for compliance are in the form of penalties for violations, and, amidst the general perceptions and fears of cybercrimes, the enforcement is increasingly widespread and severe. For instance, in May 2012 a federal appeals court upheld the conviction of a researcher at the UCLA Healthcare System for accessing the hospital’s EHR system without authorization in violation of HIPAA. This was the first person to receive a (four-month) prison sentence for violating HIPAA privacy laws by merely snooping into medical records on individuals for academic purpose with no known personal gains. This example highlights the
increased enforcement of HIPAA laws, especially significant because of the low threshold for violation set by this ruling. Other violations, especially of security breaches however small, have received significant financial penalties.

In addition to securing stand-alone EHR systems against potential breaches, the security problem has become more complex because of the variety of medical devices that contain electronic patient records. The burgeoning use of mobile devices significantly increases the data security problem. Further, the implementation of HIE and other system interoperability have essentially created a vulnerable network of systems and devices, thereby increasing many fold the likelihood of security breaches. These new security challenges have seemingly called to the attention of regulators, but no specific efforts have been taken to date.

**Mobile and Electronic Health**

In the eyes of the consumers, mobile and electronic health (eHealth and mHealth) is perhaps the fastest growing segment of HIT. The medical mobile device industry is burgeoning, and the number of healthcare mobile apps in iTunes Apps Store topped 240 in early 2014 ([https://itunes.apple.com/us/genre/ios-medical/id6020](https://itunes.apple.com/us/genre/ios-medical/id6020)). Many apps are popular even among healthcare providers (Whalen 2014). Some of those devices and apps are stand-alone, while others interface with other HIT systems such as EHRs.

Despite mHealth’s explosive growth in popularity and potential impact on the overall healthcare system, there have not been concerted government efforts of regulation. By default and largely due to legacy, the U.S. Food and Drug Administration (FDA) regulates all medical devices, and their regulatory authority is extended to cover some medium- and high-risk mobile apps, defined as those intended to be used as an accessory to a regulated medical device or transforming a mobile platform into a regulated medical device ([http://www.fda.gov/medicaldevices/productsandmedicalprocedures/connectedhealth/mobilemedicalapplications/default.htm](http://www.fda.gov/medicaldevices/productsandmedicalprocedures/connectedhealth/mobilemedicalapplications/default.htm)). It has issued a guideline for such regulations (FDA 2013). However, there has been no specific linkage of FDA’s regulatory guidelines for mobile and electronic health with either the regulations of EHR, HIE, and other technologies, which apps and devices may interface with, or those of security and privacy. The lack of coordinated regulatory approach in this area can be a growing concern for consumers and healthcare providers alike.

**Conclusion**

At first glance, regulations in the U.S. cover all five key areas of HIT, as discussed above. In some cases—particularly, EHR implementation under HITECH Act and security and privacy rules governed by HIPAA—the initial installment of regulations was extensive and substantial. However, it is clear to even a casual observer that such regulations are fragmented, driven mostly by specific technologies and regulatory history instead of overall policy goals. Many individual agencies—CMS, HHS, FDA, NIST, and so on—have their hands on certain parts of HIT, and it does not appear that the policies are well-matched. We believe that the lack of goal-driven policies and overall regulatory clarity may run the risk of ultimately hindering the growth of HIT. In the evolving socio-technical system of healthcare, a coordinated approach to HIT policy and regulation can be more effective to spur innovations and reach the ultimate goal of patient-centered care.

**REFERENCES**


