Health Care Reform and the Internet

Patricia MacTaggart[1] and Stephanie Fiore[2]

[1] Lead Research Scientist,
The George Washington University,
Department of Health Policy,
Washington, DC, United States of America
Patricia.mactaggart@gwumc.edu
[2] Research Assistant,
The George Washington University,
Department of Health Policy,
Washington, DC, United States of America
Stephanie.fiore@gwumc.edu

Abstract. U. S. health care delivery and administration systems have undergone transformations that create an evolving demand for health information technology (health IT) infrastructure. The successes of both U.S. Health Care reform and the use of the Internet for Health Information Technology rely on consumer/patient "trust" that information will remain private and secure and recognizing the interdependence of policy choices. Each decision is a balance between ease of use, privacy and security concerns of consumers/patients, practicality, costs and political will. Currently, U.S. stakeholders ranging from the federal government to private companies are working collaboratively to structure this balance. The U.S. opportunities and challenges of implementing a complete health IT picture in our current Health Reform and legal environment provides experiences for other countries to consider as health IT continues to develop internationally.

Keywords: Health Information Technology (health IT) Health Information Exchange (HIE), Health Insurance Exchange (HIE), privacy of protected health information (PHI), security.

1 Introduction

Health care delivery and administration systems are undergoing transformations that are dependent on and creating an expansive demand for health information technology (health IT). These transformations include monitoring diseases and health related activities at an individual and population level, coordinating care across providers and specialties, treating patients outside of the traditional face-to-face encounters, and tracking patient data through secure and reliable systems. In addition, consumers and providers expect access to real time information at the point of clinical care. Administratively, payment and data collection methodologies demand consideration of various insurance coverage types, demographics, use of quality metrics and reporting, and the use of performance incentives.

A M. Tjoa et al. (Eds.): ARES 2011, LNCS 6908, pp. 82–88, 2011.

The use of the Internet and broad adoption of health IT is growing at various rates across the U.S. and other countries, and there is a need to establish international standards and guidance. Decisions must be made balancing ease of use, privacy and security concerns of consumers/patients, practicality, costs and political will. The overall goal is determining the safest, most efficient methods for health IT implementation within an appropriate legal framework specific to each country, while also developing and adhering to standards that can be applied nationally as well as internationally.

2 Background

Health Information Technology "tools" help providers, consumers, vendors and stakeholders achieve efficient care and service delivery. Consistency and collaboration in policy development and implementation for use between regulatory agencies, participants (physicians, other providers and patients), and stakeholders is necessary to fully utilize the Internet and health IT to reach the U.S national goals of better health, better care and lower costs. [1]

One of the first steps is for patients and providers to understand the terminology of the changing health IT environment. Every day, new terms and acronyms are created in the U.S. alone, and their meanings change over time. For example, in the U. S., electronic health records (EHRs) go across health organizations, while electronic medical records (EMRs) are within one medical facility. More importantly, U.S. providers receive "meaningful use" incentive payments for appropriate functional use of certified EHRs, but not EMRs. The national legal basis for much of U.S. Health Care Reform can be found in the American Recovery and Reinvestment Act[2] (ARRA) and the Affordable Care Act[3] (ACA). Each Act created a HIE, but the HIEs are not the same. ARRA HIEs are Health Information Exchanges with a focus on clinical information, while ACA HIEs are Health Insurance Exchanges with a focus on coverage, or payment system, Exchanges. Both use the internet and require a secure infrastructure. Both are consumer centric; however, they are not the same.

Next, it is important that patients and providers acknowledge that use of the Internet expands faster and safer movement of data, but also magnifies potential risks. Health data protection can be enhanced through encryption, role-based access and authentication when appropriately applied. In the U.S. and other countries, electronic health (e-health) information, absent of privacy and security safeguards, is at risk of disclosure through human error such as laptop thefts and inadvertent data posting on the Internet, disregard of personal information, and breaches. Additional internet challenges include cloud computing and mobile devices that collect PHI, such as smart phones, tabulate computers, laptops, and PDAs. Many devices and systems have security capability, but with an emergent system and security rules, these options are not adequately pursued. The potential impact of privacy and security breaches not only involves invasion of privacy and finances, but also the risk of flawed medical decisions with life threatening results.

In response, security countermeasures to minimize and hopefully avoid risks are being implemented at various levels in U.S. systems and standards. They include physical access controls (locks on doors and computers), administrative controls

(security and privacy training, authorization, and auditing) to technical controls (use of authentication, encryption and firewalls). (*See Figure 1*). The security process must address all the countermeasures and allow for cross-checks. At a granular level, systems must reason if an individual seeking access is permitted to view data, and if not, what is the procedure to ensure access if denied? In the internet environment, how does the system validate that the individual is the individual he/she indicates he/she is? If the individual is authorized to receive demographic data but not clinical, what are the policies and procedures in place to assure how authorization is granted and overseen? Since the data is transported, how does it remain secure during transport as well as at rest? And lastly, what is the audit trail and who is responsible for managing the process?

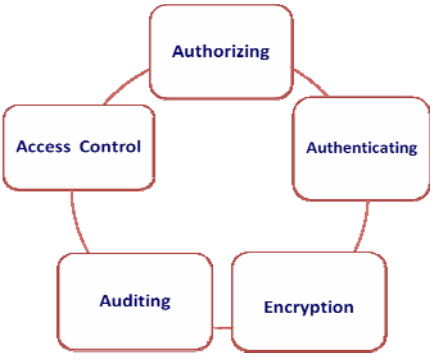

Fig. 1. Security Countermeasures for Protecting Health Information

3 Privacy and Security Themes

As expected with any field dealing with consumer's personal information, there are numerous policy and operational issues related to privacy and security in health IT. Some concerns are based on perceptions and others on reality, but to the consumer the potential impact is the same. Current key critical privacy and security themes being addressed in U.S. policies and standards are identified as follows:

A. Adequacy and Appropriateness of Current U.S. Privacy and Security Laws in an e-Health Environment

Privacy and security of health information is not a new set of concepts. In the United States, diverse federal and state laws and regulations exist that seek to address privacy and security such as HIPAA Privacy and Security Rules, Privacy Act of 1974, 42 CFR Part 2: Confidentiality of Alcohol and Drug Abuse Patient Records Regulations[4], Family Educational Rights and Privacy Act (FERPA)[5], Gramm-Leach-Bliley Financial Act[6], Federal Information Security Management Act of 2002 (FISMA)[7] and Genetic Information Nondiscrimination Act of 2008 (GINA)[8]. U.S. policy makers must examine if existing laws and regulations are appropriate and necessary for the evolving e-health environment. For example, 42

CFR Part 2 regulations, related to confidentiality of alcohol and drug abuse patient records, was developed prior to a time when chemical dependency was considered a part of health care services.

While the examples are U.S. specific, the issues are the same for any country. For example, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the European Union's Directive on Data Privacy (EU Directive) are both known for their strict regulations and potential burdens that limit flow of patient and consumer information. Privacy and security laws need to be reviewed to determine what is missing, what is no longer relevant and what amendments may be necessary due to the transformation of health care and evolution to "e-everything".

A public demand for enforcement when breaches occur will dictate further development, clarifications and modifications to existing language. Two changes that have already had significant positive impact in the U.S. are: 1) changes by Drug Enforcement Administration (DEA) related to two-factor authentication for prescribing controlled substances that make e-prescribing more viable and 2) Meaningful Use and Certification Criteria Stage 1 Privacy and Security measurements and provider attestation of a security risk assessment.

B. Consent

There are significant legal and consumer related considerations related to consent. For example, the U.S. HIPAA Privacy Act sets forth rules governing the use and disclosure of protected health information (PHI) by "covered entities" defined as health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with a covered transaction, such as submitting a health care claim to a health plan[9]. HIPAA[10] establishes the national minimum compliance framework, but states within the U.S. can and have expanded the legal provisions in areas of concern to their constituents. In addition, implementation and enforcement varies across states. Consent implementation issues relate to when and how often consent must be granted, the use of verbal or written consent, and the ability of patients to consent to the inclusion or exclusion of their personal health information. . In the U.S, legal requirements related to consent vary by the patient's age (adult or child), status (youth or emancipated adult), location of service (school or medical facility), type of service (behavioral health or substance use treatment) and purpose (secondary use of data or treatment). In addition, U.S policies include additional parameters related to disclosure and re-disclosure related to substance use treatment.

Consent implementation issues are further complicated when certain services can be categorized different ways, such as pharmaceuticals used for behavioral health could be categorized as either a pharmaceutical or a mental health service. The consent requirements vary depending on the categorization.

C. Use of Data for Treatment

Data must be "near real-time," actionable, valid and credible to be of value to providers. Data that does not easily and quickly provide accurate information has limited value. Factors that affect the transformation of data into actionable information include the security of the data in storage and transmission, standardization of terminology and

transmission systems, use of structured versus unstructured (free-text) data, access controls and the potentiality of "gaps" in vital data because of legal or consumer barriers that may result in liability concerns.

D. Use of Data Beyond Treatment

Additional and broader patient concerns arise related to secondary use of data for functions other than clinical care. This includes public health purposes such as epidemiological monitoring, administrative functions and quality improvement efforts. For example, access to eligibility and enrollment into public or private health care coverage is important for appropriate cost-covered treatment in the U.S. and can decrease the administrative burden on consumers. It can can also be useful for focusing quality improvement efforts and measuring quality results. The existing U.S. policy issue is whether the data must be de-identified when used for a secondary purpose.

E. Identity Management

A sensitive privacy and security issue currently being debated in the U.S. is the use of a national unique patient identifier. Concerns include increased patient privacy risks related to the ability to secure information about individual, fears of personal data tracking, implementation related issues (connecting to existing records), and cost when other alternatives might meet most of the needs. However, the cost of not implementing a national patient identifier has also had an impact as significant dollars and time are spent on identifying correct patient data.

From an emergency care perspective, efficient information access saves money by reducing unnecessary testing and admissions, but more importantly it aids physician care decisions. Ensuring that accurate information about the specific individual is easily accessed is very important. This is a critical policy area where the solution is a balance between accessibility to critical information while avoiding inappropriate access or disclosure of personal information.

F. Operational Requirements

As with any new area of development, there are known requirements and unknown areas to explore. Providing quick and consistent guidance regarding operational requirements will make implementation and ongoing use feasible for large and small users alike. Security questions remain regarding strength of authentication; when, with whom, and how to use digital credentials, and types of transactions to be authenticated.

Critical to efficient execution in the U.S. is intra- and inter- state consistency through mechanisms such as uniform laws, model acts, regulatory action, and reciprocity laws. One source for U.S. uniformity is the National Health Information Network (NHIN) DURSA agreement. The NHIN DURSA agreement provides standardized language related to responsibilities regarding privacy and security controls linked to malicious software; privacy and security rules; breach notification and action; oversight of technology, and compliance with laws.

International workgroups such as the Joint Initiative on SDO Global Health Informatics Standardization continue to develop standards and address issues that arise with the shift to increased health IT. The council aims for international standardization and to make all standards available through the ISO 2000 certification process, which is continually updated to meet changing needs and safety concerns. This internationally available certification process for IT systems, similar to the NHIN DURSA agreement in the U.S., encourages consistency for products in the market. However, these standards meet the challenges of enforceability and adhering to a broad range of country laws.

4 Discussion

In the U.S., the technical architecture and capability to address privacy and security issues exists and is being actively addressed. Health IT implementation, in any country, also demands the technical capacity to identify and separate sensitive health information, and to differentiate information according to type, data source and patient. The ability to segment and manage data is technically feasible; however, the demands on technology are complex, costly, and dependent on the granularity (consent by data type) required. For example, in current U.S. systems, access controls can be based on different variables (user, role, location, and group) or be rule-based. The rule-based provides greater flexibility moving forward, but it also requires a complete understanding and agreement on the legal and policy framework, the technical and operational business rules and guidance, and sufficient human and financial resources to assure correct implementation and ongoing compliance.

Implementation additionally involves the more difficult task of developing systems that may potentially integrate on an international scale, while concurrently assessing more local policies and challenges. An example of a current health IT challenge in the U.S. is that due to existing U.S. laws, the most difficult population to address is adolescents. To assure their health care needs are not ignored or disenfranchised, health IT infrastructure must have the ability to address variations in state laws regarding minor consent and definitions of “emancipated”. The system must also segment adolescent health records to avoid unauthorized disclosure through tagging all data related to a procedure to which a minor has consented, recording the related minor consent status in a structured field, and transmitting minor consent status and information tags. To add to the complexity, providers serving teens in foster care may release “confidential” HIV-related information to an authorized foster care agency, without permission, but are not required according to existing law.[11] Foster care agencies, however, must release any HIV-related medical information to prospective foster or adoptive parents, but also safeguard this information from disclosure to others. Similar to perplexities created by U.S. laws established prior to the expansion of health IT, other countries may have also or will soon need to reassess existing laws and standards when implementing health IT practices. It is anticipated that countries positive, and negative, experiences may be shared to provide examples of practices to avoid or implement while developing health IT systems.

5 Conclusion

As health IT evolves and the U.S. health care reform moves forward, decisions will need to be made on when to enforce existing or create new policies, especially those guiding privacy and security. Providers must adjust workflow related to obtaining and managing consent and data systems. Consumers and patients will need to understand the vast changes to their own health care delivery and administration, and conflicting interests of stakeholders will need to be balanced to get to a sustainable, reformed health care and information technology system. Throughout these advancements, patient privacy and security must remain at the forefront of every decision as they are essential to keeping the system credible, trusted and operating. The current experiences of the U.S. health IT evolution and lessons learned from challenges such as reviews of privacy and security laws, consent and related legal issues, use of data for treatment and beyond and identity management, combined with other international experiences, can help guide future formation of international health IT standards related to privacy and security.

References

[1] Berwick, D.: Achieving Better Care, Lower Costs: Dr. Berwick's Message. Center for Medicare and Medicaid Services [Video file] Video posted to, http://www.youtube.com/watch?v=YvTAyGoBe7Q (April 21, 2011)
[2] American Recovery and Reinvestment Act. Public Law 111-5 (2009)
[3] Patient Protection and Affordable Care Act. Public Law 111-148 & 111-152 (2010)
[4] Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. pt. 2 (2009). These regulations were promulgated pursuant to the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970, Pub. Law 91-616, 84 Stat. 1848, and the Drug Abuse Office and Treatment Act of 1972, Pub. L. No. 92-255, 86 Stat. 65. The rule-making authority granted by both statutes relating to confidentiality of records can now be found at 42 U.S.C. § 290dd-2 (2006)
[5] The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR pt. 99 (1974)
[6] Gramm-Leach-Bliley Financial Modernization Act. Public Law 106–102 (1999)
[7] E-Government Act, H. R. 2458—48 (2002)
[8] Genetic Information Nondiscrimination Act (GINA), § 102, 201, 203, 122 Stat. 894, 908-909 (codified at 42 U.S.C.A. § 300gg-1, 2000ff-2 (West 2009))
[9] Public Welfare. 45 C.F.R. § 160.103 (2009)
[10] Health Insurance Portability and Accountability Act. Public Law 104-191 (1996)
[11] Five Rivers Child Care Ltd. Privacy Statement No. 49242 (2010), Accessed from, http://www.five-rivers.org/privacy-policy.asp