Healthcare Reform and Medical Data Security and Privacy

Patricia MacTaggart
The George Washington University

Stephanie Fiore
The George Washington University

Report GW-CSPRI-2010-1

December 13, 2010

Abstract

U.S. health care delivery and administration have undergone transformations that create an expansive demand for health information technology. The concepts put forth in health care reform are reliant on an evolving health information technology infrastructure and the successes of both are dependent on consumer/patient "trust". Every action is interdependent. Each decision is a balance between ease of use, privacy and security concerns of consumers/patients, practicality, costs and political will. The goal is finding the best balance within an appropriate legal framework at the state and federal level so the pieces fit into one complete picture when implemented.

Work supported by the Office of the Vice President for Academic Affairs and the School of Engineering and Applied Science of The George Washington University

Healthcare Reform and Medical Data Security and Privacy

Patricia MacTaggart
The George Washington University

Stephanie Fiore
The George Washington University

Introduction

Health care delivery and administration are undergoing transformations that are dependent on and creating an expansive demand for health information technology (HIT). Evolving health delivery mechanisms include approaches beyond face-to-face encounters. Consumers and providers expect access to real time information at the point of clinical care. Administratively, payment methodologies demand consideration of demographics, use of quality metrics and reporting, and the use of performance incentives.

The need for clear guidance in health information technology is real. Decisions must be made balancing ease of use, privacy and security concerns of consumers/patients, practicality, costs and political will. The overall goal is finding the safest, most efficient methods for HIT implementation within an appropriate legal framework at the state and federal level.

Background

Health Information Technology is a "tool" to help providers, consumers, vendors, and stakeholders who are simultaneously entering this new and evolving environment. Consistency and collaboration between regulatory agencies, participants (physicians, other clinicians and patients), and stakeholders is necessary to fully utilize HIT to reach better health, better care, and lower costs.

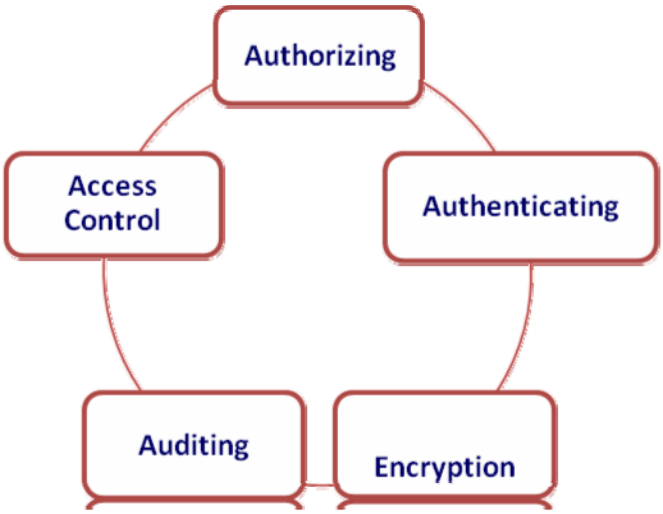
One of the first steps is for patients and providers to understand the terminology of the changing HIT environment. Every day, new HIT terms and acronyms are created and their meanings change over time. For example, EHRs are electronic health records that go across health organizations, while EMRs are electronic medical records within one medical facility. More importantly, providers received "meaningful use" incentive payments for EHRs, but not EMRs. The American Recovery and Reinvestment Act[i] (ARRA) and the Affordable Care Act[ii] created different forms of HIEs. ARRA HIEs are Health Information Exchanges, while Affordable Care Act HIEs are Health Insurance Exchanges.

HIT expands the potential for faster, safer movement of data, but also magnifies potential risks. HIT can enhance health data protection through encryption, role-based access and authentication

when appropriately applied. e-Health information, absent of privacy and security safeguards, is at risk of disclosure through human error (laptop thefts and inadvertent data posting on the Internet) and disregard of personal information (breaches). The potential impact is not only invasion of privacy and finances, but also the risk of wrong medical decisions with life threatening results.

In response to the risks, security countermeasures to avoid or at least minimize security risks exist at various levels. They range from physical controls (locks on doors and computers) to administrative controls (staff security and privacy training) to technical controls (use of authentication and firewalls).

Figure 1: Security Controls



Key Critical Privacy and Security Policy Themes

There are numerous policy and operational issues related to privacy and security in the HIT area. Some are based on perceptions and others are based on reality, but to the consumer the impact is the same. Current key critical privacy and security themes are identified as follows:

Adequacy and Appropriateness of Current Privacy and Security Laws in an e-Health Environment

Privacy and security of health information is not a new set of concepts. 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,[iii] Family Educational Rights and Privacy Act (FERPA),[iv] Gramm-Leach-Bliley Financial Act,[v] Federal Information Security Management Act of 2002 (FISMA),[vi] and Genetic Information Nondiscrimination Act of 2008 (GINA).[vii] Policy makers must examine if current laws and regulations are still appropriate and necessary in an e-health environment. For example, 42 CFR Part 2 regulation 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.

States and the federal government must also review their privacy and security laws to determine what is missing and what is no longer relevant because of the transformation of health care and evolution of HIT. Amendments may be necessary to accommodate changes that have resulted from the influx of HIT. A public demand for enforcement when breaches occur will dictate further development, clarification, and modifications to existing language. Two changes that have already had a significant positive impact are: 1) changes by 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.

Consent:

There are significant legal and consumer related considerations related to consent. The 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.[viii] HIPAA[ix] establishes the national minimum compliance framework, but states 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 to consent to stay in (opt-out) rather than consent to stay out (opt-in). 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, there are additional parameters related to disclosure and re-disclosure related to substance use treatment.

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

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 practical information include the security of the data in storage and transmission, standardization of terminology and transmission, 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.

Use of Data beyond Treatment

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

Identity Management

A sensitive privacy and security issue is the use of a unique patient identifier. Concerns range from increased patient privacy risks related to the ability to secure information about an individual to fears of what it could lead to ("big brother effect") to implementation related issues (connecting to existing records and cost when other alternatives might meet most of the needs). However, the cost of not implementing patient identifiers also has an impact as significant dollars and time are spent on identifying patients. It is a big expense to get accurate data to the provider at the right time, in a useable format, to assure efficient and effective health care delivery.

State Health Information Exchanges require a patient identifier for identity management. State Health Insurance Exchanges require the same, as do care providers. From an emergency room perspective, information access saves money by reducing unnecessary testing and admissions, but more importantly, it helps physicians make improved decisions and save lives. 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 use of personal information.

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 execution is intra- and inter- state consistency through mechanisms such as uniform laws, model acts, regulatory action, and reciprocity laws. One source for 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.

Discussion:

The technical architecture and capability to address privacy and security issues exists. 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, 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 demands the technical capacity to identify and separate sensitive health information, differentiate information according to type (HIV), data source (school), and patient. One of the most difficult, heterogeneous populations to address is adolescents. To assure adolescents' health care needs are not ignored or disenfranchised, the HIT 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 to do so.[x] Foster care agencies, however, must release any HIV-related medical information of which they have knowledge to prospective foster or adoptive parents, but also safeguard this information from disclosure to others.

Conclusion:

As HIT evolves and 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. Consumers and patients will need to understand the vast changes to their own health care delivery and administration, and conflicting interests 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.

[i] American Recovery and Reinvestment Act of 2009. (Public Law 111-5).
[ii] Patient Protection and Affordable Care Act of 2010. (Public Law 111-148 & 111-152)
[iii] 42 C.F.R. Part 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 rulemaking authority granted by both statutes relating to confidentiality of records can now be found at 42 U.S.C. § 290dd-2 (2006).
[iv] The Family *Educational Rights and Privacy Act* (*FERPA)* of 1974 (20 U.S.C. § 1232g; 34 CFR Part 99
[v] *Gramm-Leach-Bliley* Financial Modernization Act of 1999. (Public Law 106 – 102)
[vi] http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
[vii] GINA §§ 102, 201, 203, 122 Stat. at 894, 908-909 (codified at 42 U.S.C.A. §§ 300gg-1, 2000ff-2 (West 2009))
[viii] 45 C.F.R. § 160.103 (2009).
[ix] Health Insurance Portability and Accountability Act of 1996. (Public Law 104-191).
[x] http://www.five-rivers.org/privacy-policy.asp