Journal of Diabetes Science and Technology
Volume 4, Issue 3, May 2010

COMMENTARY

The Secret to Health Information Technology's Success within the Diabetes Patient Population: A Comprehensive Privacy and Security Framework

Sheel M. Pandya, J.D., M.P.H.

Abstract

Congress made an unprecedented investment in health information technology (IT) when it passed the American Recovery and Reinvestment Act in February 2009. Health IT provides enormous opportunities to improve health care quality, reduce costs, and engage patients in their own care. But the potential payoff for use of health IT for diabetes care is magnified given the prevalence, cost, and complexity of the disease. However, without proper privacy and security protections in place, diabetes patient data are at risk of misuse, and patient trust in the system is undermined. We need a comprehensive privacy and security framework that articulates clear parameters for access, use, and disclosure of diabetes patient data for all entities storing and exchanging electronic data.

J Diabetes Sci Technol 2010;4(3):740-743

Federal Investment in Health Information Technology

Health information technology (IT), which includes electronic medical records and electronic health information exchange, has the potential to revolutionize our health care system by improving quality of care, reducing costs, and empowering patients to become more involved in their own health care. Realizing its potential benefits, Congress made an unprecedented investment in health IT—approximately $46.8 billion—as part of the American Recovery and Reinvestment Act of 2009 (ARRA) (also known as the federal stimulus package), which President Obama signed into law on February 17, 2009.[1] Consequently, clinicians and hospitals are likely to adopt health IT (through financial incentives) at a faster pace over the next several years.

Potential Benefits of Health Information Technology within the Diabetes Patient Population

In 2007, diabetes affected 23.6 million people in the United States (7.8% of the population) at a cost of $174 billion.[2] Diabetes also requires a high level of

Author Affiliation: Center for Democracy and Technology, Washington DC

Abbreviations: (ARRA) American Recovery and Reinvestment Act of 2009, (FIP) fair information practice, (HIPAA) Health Insurance Portability and Accountability Act, (IT) information technology, (PHR) personal health record

Keywords: American Recovery and Reinvestment Act of 2009, comprehensive privacy and security framework, diabetes, health information technology, health privacy, patients

Corresponding Author: Sheel M. Pandya, J.D., M.P.H., Center for Democracy and Technology, 1634 I Street, NW, Suite 1100, Washington DC 20006; email address spandya@cdt.org

patient management and coordination of care, because it is frequently associated with comorbid conditions, requires multiple medications in its management, and involves monitoring several measures of disease control.[3] As a result, diabetes patients (and their providers) could significantly benefit from health IT adoption.

In fact, applications of health IT are already available to diabetes patients and providers in the management and treatment of the disease. For example, diabetes patients measure their blood glucose levels almost every day or several times during the day. New technology allows these patients to upload their glucose data directly from glucose meters to computer-based management programs, where the data can be stored or shared with their providers who can then read the data and send back recommendations. Likewise, diabetes patients can manually enter their health data, including information about diet and exercise, into a smart phone or an online personal health record (PHR) and store or send these data to whomever they choose. Diabetes patients can also utilize third party applications, including medication and disease-monitoring tools, through their smart phones or PHRs to help manage their disease.

Telemedicine is a rapidly developing application of health IT to the management and treatment of diabetes. It involves the use of telecommunications to transmit patient data (in a timely way) into an electronic medical record and remote interpretation of these data by a provider (sometimes with the help of decision-support software) for follow-up and preventative purposes.[4] Telemedicine allows providers to monitor diabetes patients remotely between in-person visits. It is especially well suited to treating diabetes (compared to other diseases), because effective diabetes treatment requires ongoing interpretation of several types of data (e.g., glucose, blood pressure, and behavioral data) that can be measured by diabetes patients at home. The end goal for telemedicine is to foster productive interactions between patients and providers to further achieve improved quality of care and lower costs.[4]

Need for a Comprehensive Privacy and Security Framework to Protect Diabetes Patient Data

Undoubtedly, health IT has the ability to transform how diabetes patients manage their disease and how providers care for them. But the uses of health IT among these patients and providers also raise serious privacy and security concerns.[5,6] Without proper privacy and security protections in place, diabetes patient data are at risk of inappropriate or unauthorized access or misuse, and public trust in the health IT system is significantly undermined.

Although a large majority of the public wants electronic access to their health data (for both themselves and their providers), a significant portion of the public also consistently expresses concern over the privacy of these data.[6] These concerns are only fueled by large-scale, widely publicized privacy and security breaches of patient data. (Examples of data privacy and security breaches available from http://www.washingtonpost.com/wp-dyn/content/article/2008/04/09/AR2008040903680.html; http://www.nytimes.com/2006/05/23/washington/23identity.html?ex=1306036800&en=eb1c02a63fedca31&ei=5090&partner=rssuserland&emc=rss; and http://datatheft.berkeley.edu/.) Research shows that patients will practice privacy-protective behaviors—such as avoiding seeing a doctor or withholding information relevant to their care—if they are unsure their personal information will be adequately protected.[6–8] The consequences of this could be significant: the quality of patient care could suffer, the ability of providers to diagnose and treat patients accurately may be impaired, and the cost of health care could escalate as conditions are treated at a more advanced stage.[6–8] Failure to address patient privacy concerns could be particularly harmful if diabetes patients are reluctant to seek care or have their health data shared for care purposes.

To better protect diabetes patient data and build trust in the health IT system, we need a comprehensive privacy and security framework in place that articulates clear parameters for access, use, and disclosure of patient data for all entities engaged in actively storing and managing electronic health data. In fact, a framework for health IT already exists in the form of the generally accepted "fair information practices" (FIPs) that have been used to shape policies governing personal data use in several contexts. One version of FIPs is the federal Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, which governs the access, use, and disclosure of personal health data by "covered entities," including health care providers and plans.

While there is no single formulation of FIPs, the common framework developed by the Markle Foundation's Connecting for Health Initiative implements core privacy principles, adopts trusted network design characteristics, and establishes oversight and accountability mechanisms.[9] This framework acknowledges the role that technology

can play in protecting privacy and can help guide policymakers, key regulatory agencies, and developers of health IT systems in establishing appropriate privacy and security protections for personal health data online.

The principles are as follows:

Openness and Transparency: There should be a general policy of openness about developments, practices, and policies with respect to personal data. Individuals should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides.

Purpose Specification and Minimization: The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes or others that are specified on each occasion of change of purpose.

Collection Limitation: Personal health information should only be collected for specified purposes and should be obtained by lawful and fair means and, where possible, with the knowledge or consent of the data subject.

Use Limitation: Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.

Individual Participation and Control:

- Individuals should control access to their personal health information and should be able to obtain information about whether or not the entity has data relating to them from each entity that controls personal health data.
- Individuals should have the right to
    - Have personal data relating to them communicated within a reasonable time (at an affordable charge, if any) and in a form that is readily understandable,
    - Be given reasons if a request (as described earlier) is denied and be able to challenge such denial, and
    - Challenge data relating to them and have it rectified, completed, or amended.

Data Integrity and Quality: All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and current.

Security Safeguards and Controls: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.

Accountability and Oversight: Entities in control of personal health data must be held accountable for implementing these information practices.

Remedies: Legal and financial remedies must exist to address any security breaches or privacy violations.

Fortunately, the timing for putting a comprehensive framework in place could not be more favorable, given the confluence of developments in both health care reform and health IT. After a year-long debate in Congress over health care reform, President Obama signed into law the Patient Protection and Affordable Care Act on March 23, 2010.[10] Combined with the Health Care and Education Reconciliation Act of 2010[11] amendments, this legislation leverages health IT to achieve health care reform goals, including improving health care quality and reducing costs. The health IT provisions in the new law are intended to build upon the foundation laid by ARRA, which (in addition to a significant federal investment in health IT) includes the most important improvements in health privacy that we have seen in a decade, including substantive changes to HIPAA privacy and security rules. ARRA represents an important step forward in achieving a comprehensive privacy and security framework, but more work needs to be done. Regulation and additional guidance are needed to flesh out the statutory requirements in ARRA, and better enforcement of the privacy rules is necessary.

Additionally, a set of rules is needed for PHRs and other Internet-based services that operate outside of the traditional health care system. Currently, there is no consistent regulatory framework in place for PHRs.[12] If they are not regulated by HIPAA, which is the case for most PHRs, patient privacy may be protected only by the PHR provider's privacy and security policies (and potentially under certain state laws that apply to uses and disclosures of certain types of data).[12] Regardless of what types of entities are offering PHRs, they ought to be governed by a consistent and meaningful set of privacy and security policies.[12] Fortunately, ARRA provides opportunities to advance such a consistent approach. In particular, the U.S. Department of Health and Human Services, in consultation with the Federal Trade Commission, is required to make recommendations

to Congress for privacy and security requirements for PHR providers and related entities that are not covered by HIPAA.[1] Moving forward, policymakers will need to continue to pay attention to privacy and security issues in order to build a strong foundation of trust in health IT.

Conclusion

Health IT adoption is already underway within the diabetes patient population and in the health care system as a whole. Furthermore, adoption will likely ramp up as more clinicians and hospitals qualify for financial incentives under ARRA. Attempting to institute privacy protections retroactively, and restoring public trust that has been significantly lost, is infinitely more difficult than building it in from the start. The time is now to establish effective, comprehensive privacy and security protections for personal health data online.

References:

1. American Recovery and Reinvestment Act of 2009. Public Law 111-5. Signed February 17, 2009.
2. U.S. Department of Health and Human Services. Centers for Disease Control and Prevention. National diabetes fact sheet, 2007. http://www.cdc.gov/diabetes/pubs/pdf/ndfs_2007.pdf.
3. Wyne K. Information technology for the treatment of diabetes: improving outcomes and controlling costs. J Manag Care Pharm. 2008;14(2 Suppl):S12–7.
4. Klonoff DC. Using telemedicine to improve outcomes in diabetes: an emerging technology. J Diabetes Sci Technol. 2009;3(4):624–8.
5. Markle Foundation, Lake Research Partners, American Viewpoint. Survey finds Americans want electronic personal health information to improve own health care. November 2006. http://www.markle.org/downloadable_assets/research_doc_120706.pdf.
6. California Healthcare Foundation, Forrester Research, Inc. National consumer health privacy survey 2005. November 2005. http://www.chcf.org/topics/view.cfm?itemID=115694.
7. Goldman J. Protecting privacy to improve health care. Health Aff (Millwood). 1998;17(6):47–60.
8. Goldman J, Hudson Z, Health Privacy Project, California Healthcare Foundation. Promoting health/protecting privacy: a primer. January 1999. http://www.chcf.org/topics/view.cfm?itemID=12502.
9. Markle Foundation. Connecting for Health. http://www.connectingforhealth.org/.
10. Patient Protection and Affordable Care Act. Public Law 111-148. Signed March 23, 2010.
11. Health Care and Education Reconciliation Act of 2010. H.R. 4872. Public Law 111-152. Signed March 30, 2010.
12. Center for Democracy and Technology. Testimony of Deven McGraw before the National Committee on Vital and Health Statistics. Hearing on personal health records. June 9, 2009. http://www.cdt.org/testimony/testimony-deven-mcgraw-ncvhs.