ISSUE BRIEF NQF

National Quality Forum

NO. 18
JANUARY 2010

Privacy: From Barrier to Enabler of Health Information Technology (HIT)

EXECUTIVE SUMMARY

Our 21st century health system relies on 19th century methods of recording and transmitting data. The usual result is that a significant portion of information in the patient's record is missing or incomplete, or can be interpreted out of context, leading to the risk of incorrect conclusions. To improve the quality of medicine and minimize the possibility of adverse outcomes, healthcare advocates place great hope in the potential of HIT. HIT—featuring but not limited to electronic health record (EHR) systems—today is considered foundational to the transformation of the U.S. health system.

Barriers to widespread HIT adoption remain, and the federal government is taking steps to address many of them. But the challenge of privacy and security is of special significance because it is not only a legal and regulatory issue but also a cultural issue that directly impacts consumers' relationships with their doctors, hospitals, insurers, and with the government. The privacy dimension carries additional weight because of the effect it may ultimately have on care itself; if patients do not fully trust a system, they may engage in "privacy protective" behaviors, the risks of which can be seriously or even deadly.

But, American consumers have demonstrated that they are willing to trust systems, including technology-based systems, if they believe that reasonable steps are taken to use their personal information judiciously and if the benefit to using such systems is clear. Healthcare providers and other stakeholders must prove their worth by demonstrating utmost respect to privacy and security and by articulating the value proposition. If they do, then privacy ceases to act as a barrier to adoption of EHRs and in fact enables it—because consumers trust it and look forward to a tangible benefit. The security of these systems becomes assumed and therefore a non-issue, and—like credit cards or automated teller machines—it becomes easier to use an HIT-enabled system than to avoid it. For this to occur successfully, the healthcare field must adopt a culture of privacy and work with the government to ensure that the legal and regulatory oversight structure remains up to date.

I. Introduction: The Foundational Importance of Health Information Technology

Good healthcare depends on good information. That information can include a patient's diagnosis, illness history, family history, recent test results, or information about a new treatment or intervention that could save a life. As much as any modern endeavor, healthcare demands that the right information about the right person be delivered—in usable form—to the right place at the right time.

Unfortunately, our 21st century health system relies on 19th century methods of recording and transmitting data, with an over-reliance on written records and, sometimes, clinicians' memories. The usual result is that a significant portion of information in the patient's record is missing or incomplete, or can be interpreted out of context, leading to the risk of incorrect conclusions. The outcome can be disastrous.

"Nothing could be more important than how we manage health information," says David Blumenthal, MD, MPP, the Obama Administration's national coordinator for health information technology (HIT). "Information is the lifeblood of

➲ *Continued on page 2*

medical practice. It truly sustains and supports practice, and makes it possible for practice to occur in a science-based way."

To improve the quality of medicine and minimize the possibility of adverse outcomes, healthcare advocates place great hope in the potential of HIT. HIT—featuring but not limited to electronic health record (EHR) systems—today is considered foundational to the transformation of the U.S. health system.[1]

HIT-enabled content and transactions hold the promise of making important healthcare information more readily available to those who need it. If they are implemented with careful attention to workflow and content needs, EHR systems will appreciably improve the safety, effectiveness, and efficiency of American healthcare, leading to widespread and sustainable quality improvement. Such systems will support clinical decisions, grant patients and clinicians access to health records, and improve the accuracy of those records; seamlessly integrate clinical and payment functions; and facilitate the collection, reporting, and analysis of quality data.

"HIT is not a panacea. But its potential to rationalize and enable redesign of the delivery of healthcare in the United States, and thereby foster a rapid improvement in the quality of care delivered to millions of Americans, is vast," says Janet M. Corrigan, PhD, MBA, president and CEO of the National Quality Forum (NQF). "For those who are seeking to improve the quality of American healthcare, HIT—particularly EHR systems—is the cornerstone on which the entire enterprise is built."

Federal policymakers repeatedly have signaled their recognition of HIT's importance, most recently with the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) portion of the American Recovery and Reinvestment Act.[2] Through HITECH, the federal government is encouraging and funding the rapid development and adoption of EHR systems.

Separately, many healthcare organizations are engaged in industry collaborations, public-private partnerships, and other endeavors to pave the way for rapid HIT adoption. These include the Certification Commission for Health Information Technology,[3] an independent not-for-profit organization that certifies EHR systems; the Healthcare Information Technology Standards Panel,[4] a public-private partnership seeking to harmonize and integrate standards that will meet clinical and business needs for sharing information among organizations and systems; and the National eHealth Collaborative,[5] successor to the American Health Information Community, which is working on a number of initiatives critical to a nationwide electronic health information network.

Spurred by increased federal incentives, U.S. healthcare providers are devoting resources to modernizing their information infrastructure. From large multi-state hospital systems serving millions of patients to small physician practices, providers are adopting EHR systems and other HIT products (e.g., computerized physician order entry, barcode-enabled medication administration). Many of these HIT adoption efforts remain in their infancy and may not show results for several years, but their ultimate value, when appropriately implemented and addressing workflow, is clear.

Concurrently, NQF is engaged in a full slate of HIT-related activities. These include the endorsement, through NQF's voluntary, stakeholder-based consensus process, of nine structural measures to encourage HIT adoption by clinicians[6] and its sponsorship of the Health Information Technology Expert Panel (HITEP), which has recommended common data types, prioritized performance measures for electronic healthcare information systems,[7] proposed a Quality Data Set (QDS) framework to define electronic health information,[8,9] and successfully sponsored the creation of an electronic measure format standard that will allow future measures to address information as it is used in the EHR.[10] These efforts reflect the central role that HIT is considered to play in healthcare quality improvement.

II. Privacy: The Cultural Barrier

Barriers to widespread implementation remain, and many are well recognized. These include the adoption of technical standards so that disparate providers, payers, and systems can share information; cost, return on investment, and the value proposition; and privacy and security. Because HIT is so important to healthcare quality improvement, it is critical that quality stakeholders contribute to the resolution of these problems.

The federal government and other institutional stakeholders are addressing many of these challenges. But the latter challenge—privacy and security—is of special significance because it is not only a legal and regulatory issue but also a cultural issue that directly impacts consumers' relationships with their doctors, hospitals, insurers, and with the government.

American consumers place high value in privacy and define the concept broadly. We have a long tradition of guarding our privacy carefully, of relying on the law to safeguard it, and of deep skepticism regarding how technological developments can impact it. Many Americans consider the right to privacy to be guaranteed by the Fourth Amendment to the U.S. Constitution, which guards against unreasonable searches and seizure. In 1890, prominent attorneys Samuel Warren and Louis Brandeis famously asserted that privacy, or "the right to be let alone," was under threat from "recent inventions and business methods," necessitating the development of new legal protections.[11] Today, despite the proliferation of Internet-enabled social networking and easy public access to electronic networks, in which personal information is readily available and easily distributable electronically, consumers in the United States remain naturally protective of information about themselves and wary about its use and potential misuse.

The healthcare field is not immune from these concerns. Many Americans are reflexively mistrustful of seemingly impersonal institutional users of information and question whether such entities are worthy of their confidence. More than half of the 10,258 U.S. participants in one poll expressed privacy concerns regarding their medical records and information in 2007.[12] In another survey about online access to health records, four-fifths of respondents said they were very concerned about identity theft or fraud; 77 percent said they were very concerned about their medical information being used for marketing purposes; 56 percent were concerned about employers having access to their health information; and 53 percent were concerned about insurers gaining access to their health information.[13]

"The conversion to HIT-dependent systems of care has raised significant concerns about access to information," says Floyd Eisenberg, MD, MPH, FACP, senior vice president for Health Information Technology at NQF. "Hospitals and other providers of care already were maintaining, and in some instances sharing, this information, but only in a paper format. What many people might not realize is that, because of audit trails and strictly defined limits on who may see what information, electronic health data has the potential to be *more* secure than paper-based data, not less secure."

The privacy dimension carries additional weight because of the effect it may ultimately have on care itself. Privacy advocate Janlori Goldman, a senior policy advisor to the Center for Democracy and Technology, has identified certain "privacy-protective" behaviors in which some patients engage to protect what they perceive to be threats to their privacy if they do not fully trust the health system to provide that protection for them.[14] Such behaviors may include withholding information from a clinician; paying out-of-pocket for services that would otherwise be covered by their insurance; asking doctors to lie on official forms about their diagnosis; lying to providers; switching clinicians frequently to ensure that all of their information is not held in one place; and avoiding care altogether.

The risk of such avoidance can be serious or even deadly. If patients engage in privacy-protective behaviors, their care may suffer, clinicians' ability to diagnose and treat a condition may be impaired, and research and public health goals may be undermined.[15]

"In medicine, we depend on complete information from our patients, or at least the closest approximation of complete information as we can get," says John D. Halamka, MD, MS, chief information officer of Harvard Medical School and Beth Israel Deaconess Medical Center, Boston. "Anything less than total honesty puts patients and the public at risk. Mistrust and doubt should never interfere with the doctor-patient relationship."

III. Privacy as an Enabler to HIT Adoption

Even as HIT's potential advanced dramatically in the past decade, many policymakers have shied away from it, in part because of privacy issues. "Privacy has become the third rail for many policymakers. Nobody wants to touch it," says Deven McGraw, JD, LLM, MPH, director of the Health Privacy Project at the Center for Democracy and Technology.

But, American consumers have demonstrated that they are willing to trust systems, including technology-based systems, if they believe that reasonable steps are taken to use their personal information judiciously and if the benefit to using such systems is clear. Clear examples exist in banking, in which Americans engage in online transactions, deposit and withdraw money from automated teller machines (ATMs), and allow their paychecks to be deposited directly into their accounts; and in Internet-enabled commerce, in which Americans routinely send credit card information over networks they assume to be secure.

These industries have successfully transitioned to a modern infrastructure that transmits personal information over electronic networks because they have achieved two goals: they have persuaded the consumer public that reasonable steps are being taken to protect private information, and they have demonstrated value to consumers (e.g., financial benefit, convenience) in using electronic networks.

Similarly, healthcare providers and other stakeholders must prove their worth by demonstrating utmost respect to privacy and security and by articulating the value proposition (i.e., the quality case for why patients benefit from having their medical information stored on an EHR). If they do, then privacy ceases to act as a barrier to adoption of EHRs and in fact enables it—because consumers trust it and look forward to a tangible benefit. The security of these systems becomes assumed and therefore a non-issue, and—like credit cards or ATMs—it becomes easier to use an HIT-enabled system than to avoid it.

"The public has to trust these systems in order for them to be used," Ms. McGraw says. "If we can demonstrate that our systems are trustworthy—if we establish a culture of privacy that is every bit as strong as the culture of safety that is being nurtured within healthcare today—then we have every reason to believe that we will see rapid uptake of HIT on the part of consumers."

IV. The Culture of Privacy

Cultural shifts in healthcare are difficult to achieve—but not impossible. Regulatory and legislative action can contribute to a cultural shift, but can't achieve it alone. Such a shift demands rigorous performance measurement, consistent attention to improvement, and—perhaps most significantly—a steady leadership focus to achieve it. It takes a great deal of time and patience for inevitable setbacks. "We've been talking about a culture of safety in healthcare for well over a decade, and we are only now truly instilling such a culture broadly throughout the system," Dr. Corrigan says.

A culture of privacy demands a balance between an individual's desire for confidentiality and the development of a "learning healthcare system" in which information is routinely shared to improve the system as a whole. There is natural tension between these two competing, worthy goals. To establish a culture of privacy, several steps need to be taken, including:

1. **The development of a comprehensive privacy framework.** This needs to occur both at the broad national level and at the individual provider level. A privacy framework is a set of underlying core principles that, beyond any law, regulation, or institutional policy, guarantees that privacy is a sacrosanct concept. It places the burden on the institution, rather than on the individual, to protect that privacy and ensure that proper security measures are in place to do so. Such a framework is implied, although not explicitly stated, in existing IT efforts such as NQF's HITEP work.

2. **The clear definition of how (and where) data should be stored.** This may seem like an arcane technical matter, but consumers are stakeholders. Many consumers are profoundly uncomfortable with the concept of their information being stored on a central database, but are much more comfortable with network-to-network approaches that allow data to be stored in one place and accessed on an as-needed-and-only-as-needed basis.

3. **The resolution of legal and regulatory issues.** While the Recovery Act builds on existing federal privacy law (*see Section IV*), there is an implementation challenge ahead. There also remain significant gaps in federal laws and where they intersect with state privacy laws and regulations. Stronger laws will create a safer electronic environment for health data, which should enhance consumers' confidence.

4. **The strengthening of audit trails.** This is another seemingly esoteric issue that cuts to the heart of consumers' confidence in the security of systems. Already, electronic audit trails can indicate when any party accesses protected data, and clear violations are punishable by firing or criminal prosecution, making electronic data safer than paper-based data in some instances. Strengthening these audits will enhance consumers' confidence in HIT systems.

5. **Clarity with respect to anonymized data and "opt-out" provisions.** Quality data today are "anonymized," or stripped of personally identifying information. These data then can be reported to quality monitoring agencies (e.g., how many female Medicare beneficiaries were given aspirin at arrival for a heart attack at a hospital) or to public health agencies. Various stages of anonymizing or "pseudonymizing" (removing a name and personally identifying information but creating a pseudonym in order to report individual case studies) exist. How-ever, as quality measurement and public reporting advance, more information will be made available to the public—and third parties may use sophisticated techniques to identify data thought to be anonymized or pseudonymized. A culture of privacy demands rigorous standards regarding these data and ensuring that they are not reidentifiable (for purposes such as marketing).

"Changing culture does not happen easily, and it does not happen painlessly, but the experience in adopting a culture of safety within healthcare demonstrates that it is possible," Corrigan says. "For us to fully realize the potential of HIT, we need to approach privacy as a cultural issue and treat it accordingly."

V. Recent Federal HIT Legislation

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 has stood as landmark federal legislation governing health privacy for more than a dozen years. Its Privacy Rule provides federal protections for personal health information and gives patients rights with respect to that information. The rule also permits the disclosure of personal health information needed for patient care and for other purposes.[16]

However, Congress passed HIPAA long before any modern conception of EHR systems, personal health record (PHR) systems, online record access, or any of the other recent HIT developments emerged. These developments could radically alter how health information is recorded, transmitted, and used. Many observers consider HIPAA's privacy provisions outdated. "HIPAA was written in 1996, at a time when electronic health records were just emerging. A decade later, as we develop the standards and capabilities to share data beyond the four walls of an individual healthcare organization, the privacy rule in HIPAA is not longer sufficient to protect individual health data stored and accessed in multiple locations," says Paul Tang, MD, MS, vice president and chief medical information officer at the Palo Alto Medical Foundation, Palo Alto, CA. "The Recovery Act enhanced HIPAA in a number of ways, but more needs to be done."

Among other things, the Recovery Act is the most encompassing federal health privacy legislation since HIPAA. Health IT advocates are optimistic that the strengthened legal framework will create a safer electronic environment for health information, thus enhancing cultural acceptance of HIT.

The new provisions include changes in HIPAA enforcement and provisions to address health information held by entities other than HIPAA "covered entities" (e.g., physicians, hospitals, health plans) or "business associates."[17] Most of the provisions are to take effect in early 2010.[18]

Perhaps most significantly, the Recovery Act expands the scope of existing HIPAA privacy and security laws by applying them directly to business associates, such as Health Information Exchanges, Regional Health Information Organizations, and PHR system vendors, rather than just covered entities. This may ease the burden on covered entities to defend against violations by business associates,[19] as it shifts liability for violation from the covered entity to the business associate.

Under the Recovery Act, covered entities are now required to notify individuals if their privacy has been breached—if there has been an instance of unauthorized access, acquisition, use, or disclosure of protected health information. The sale of protected health information is specifically prohibited, except for instances such as public health purposes, research, or treatment.[20]

The Recovery Act also specifically permits criminal prosecution for violation of HIPAA privacy rules, and increases potential civil monetary penalties from $100 per violation (up to a maximum per year of $25,000) to $50,000 per violation (up to an annual maximum of $1.5 million).[21]

VI. Conclusion

The roadmap to cultural acceptance of HIT may lie with the history of the ATM.

The first prototype of an ATM was unveiled in 1939, but banks were not interested in installing them.[22] ATMs in an iteration resembling their modern form were introduced in the late 1960s in Great Britain and in the United States. By 1973, approximately 2,000 ATMs were in use in the United States,[23] but these were still connected only to individual bank branches. In 1974, the first network of ATMs was introduced, so that simple transactions (i.e., deposits, cash withdrawals) could be performed anywhere. Today, more than 1.5 million ATMs are used worldwide.[24]

The physical security of ATMs themselves, and of those delivering cash to the machines, posed the greatest initial security challenge. Quickly, however, transactional security to guard against fraud emerged as a top concern. Transactional security ultimately was imposed by data encryption and today relies on a system known as "Triple DES," a strong encryption method that protects the personal identification number as it is sent from the machine to the bank for verification.[25]

"The overwhelming majority of us use ATMs without giving a second thought to the security of the electronic transaction, and we use them because they're easier and we trust them implicitly," NQF's Dr. Eisenberg says. "ATMs expand our access to the banking system because we are no longer confined to do our banking during 'banking hours.' Similarly, EHRs and other HIT-enabled systems actually will expand consumers' access to the healthcare system, in that people will be able to engage in certain healthcare 'transactions' at the time and place of their choosing. But this will only happen when people trust the network so much that they stop thinking about it."

The healthcare quality improvement enterprise ultimately will rely on a sophisticated HIT network that collects quality data at the point of care, delivers these data to reporting entities without burdening the provider, and employs decision support technology to provide clinicians with feedback and usable advice in real time. This vision demands a highly developed national healthcare information infrastructure, full buy-in and support from provider organizations and individual clinicians, and heavy participation by consumers. Dr. Blumenthal, the national health IT coordinator, envisions a day in the near future when HIT's value is unquestioned. "HIT will at some point be as integral to medicine as the stethoscope," he says. "I don't think it will be possible to qualify as a professional without using all the tools that are available to us as professionals, and that will include HIT. I don't think that physicians will tolerate working in a setting that is not modern."

But this vision depends on consumers, who will determine the success of HIT in

NQF
National Quality Forum

NQF's mission is to improve the quality of American healthcare by setting national priorities and goals for performance improvement, endorsing national consensus standards for measuring and publicly reporting on performance, and promoting the attainment of national goals through education and outreach programs.

NQF Issue Briefs provide insight into payer, policy, and industry efforts to promote quality healthcare. The work of HITEP II was supported by the Agency for Healthcare Research (AHRQ). The 2009 Fall Conference was support in part by Bristol-Meyers Squibb and sanofi aventis. Sustaining support is provided by the Cardinal Health Foundation.

NATIONAL
QUALITY FORUM

601 13th Street NW
Suite 500 North
Washington, DC 20005
202-783-1300 Tel
202-783-3434 Fax
www.qualityforum.org

Issue Brief No. 18
January 2010

their adoption of it. While performance measurement, public reporting, and clinical decision support are critical to quality improvement, so too are privacy and consumer preference—and these needs must be balanced. Consumers have demonstrated that they will use technology-based systems to collect and transmit very personal information about themselves—but first, they have to trust it. If healthcare providers, payers, vendors, and regulators can demonstrate that they can behave responsibly with personal healthcare information, then privacy will cease to be a barrier and instead will enable adoption.

Acknowledgments

NQF staff members Floyd Eisenberg, Sarah Callahan, and Margaret Kay, with Philip Dunn and Tamara Lee, consultants to NQF, contributed to this *Issue Brief*. ●

Notes

1 National Quality Forum (NQF). *Wired for Quality: The Intersection of Health IT and Healthcare Quality.* Washington, DC: NQF; 2008.

2 American Recovery and Reinvestment Act of 2009. Available at http://www.recovery.gov/About/Pages/The_Act.aspx. Last accessed December 2009.

3 Certification Commission for Health Information Technology. Available at http://www.cchit.org/. Last accessed December 2009.

4 Healthcare Information Technology Standards Panel. Available at http://www.hitsp.org/. Last accessed December 2009.

5 National eHealth Collaborative. Available at http://www.nationalehealth.org/. Last accessed December 2009.

6 NQF. *National Voluntary Consensus Standards for Health Information Technology: Structural Measures 2008.* Washington, DC: NQF; 2008.

7 NQF. *Recommended Common Data Types and Prioritized Performance Measures for Electronic Healthcare Information Systems.* Washington, DC: NQF; 2009.

8 NQF. *Health Information Technology Automation of Quality Measurement: Quality Data Set and Data Flow.* Washington, DC: NQF; 2009.

9 NQF. *Policy Brief: HITEP II.* Washington, DC: NQF; 2009.

10 HL7. *Automating Performance Measurement Using Electronic Health Records: Health Quality Measure Format Ballot Announced.* Available online at http://www.hl7.org/documentcenter/public/pressreleases/HL7_PRESS_20090827.pdf. Last accessed December 2009.

11 Warren S, Brandeis L. The Right to Privacy. *Harvard Law Review.* December 15, 1890. Available at http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Last accessed December 2009.

12 UPI-Zogby International Poll: Concerns on Health Privacy. UPI, Feb. 21, 2007.

13 Study by Lake Research Partners and American Viewpoint, conducted by the Markle Foundation, November 2006.

14 Goldman J. Protecting Privacy To Improve Health Care. *Health Affairs,* November-December 1998:47.

15 Center for Democracy and Technology. Comprehensive Privacy and Security: Critical for Health Information Technology. Version 1.0—May 2008.

16 U.S. Department of Health and Human Services. Health Information Privacy. Available online at http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html. Last accessed November 2009.

17 Center for Democracy and Technology. Summary of the Health Privacy Provisions in the 2009 Economic Stimulus Legislation. April 29, 2009.

18 American Medical Association. H.R. 1, the "American Recovery and Reinvestment Act of 2009," Explanation of Privacy Provisions. Available at www.ama-assn.org/ama1/pub/upload/mm/399/arra-privacy-provisions.pdf. Last accessed November 2009.

19 *Ibid.*

20 Center for Democracy and Technology. Summary of the Health Privacy Provisions.

21 *Ibid.*

22 ATM Machine History. http://www.ehow.com/about_5052349_atm-machine-history.html. Last accessed December 2009.

23 Timeline: The ATM's History. http://www.atm24.com/newssection/industry%20news/timeline%20-%20the%20atm%20history.aspx. Last accessed December 2009.

24 ATM Machine History.

25 Diebold Inc. *ATM Fraud and Security White Paper.* September 2002. Available at http://buy.cuna.org/download/diebold_fraudpaper.pdf. Last accessed December 2009.