STATEMENT OF

DAVID MERRITT

PROJECT DIRECTOR,
CENTER FOR HEALTH TRANSFORMATION*

BEFORE THE SENATE JUDICIARY COMMMITTEE

TUESDAY, JANUARY 27, 2009

Chairman Leahy, Senator Specter, and members of the committee:

Thank you for the opportunity to testify about how to modernize our healthcare system through information technology while protecting patient privacy.

Information about our health and healthcare is by far the most sensitive data a person owns. From chronic conditions to medications to genetic makeup, our personal health information reveals intimate details about who we are, what we do, and what we may be like in the future. Thus, protecting our privacy and confidentiality is a principle that simply cannot be compromised.

However, as the pace quickens to modernize healthcare through information technology, such as through the adoption of electronic health records, there is a growing tension between protecting personal data and having instant access to it when it is needed.

On the one hand, having real-time access to personal health information can often mean the difference between life and death. On the other hand, the loss of such sensitive data to outsiders, especially those with nefarious or self-interested intentions, can have disastrous and long-term consequences.

The Congress has started an important conversation of how policy can help balance progress and privacy: Progress toward building an electronic health system and protecting the privacy of those who are part it.

This must be done exactly right. For if there are onerous restrictions or cumbersome administrative burdens on physicians, health systems, and other providers, then they will not adopt new technology, and patients will suffer by not

---

* The Center for Health Transformation, founded and led by former Speaker of the House Newt Gingrich, is a collaboration of leaders dedicated to the creation of a 21st Century Intelligent Health System that saves lives and saves money for all Americans. For more information on the Center and our Health Information Technology project, please visit www.healthtransformation.net.

receiving the best possible care. If restrictions on electronic data exchange are too excessive, new breakthroughs that can found by researching de-identified patient data will not happen. The widespread adoption of information technologies and the use of new research tools are desperately needed to bring our healthcare system out of the Stone Age. Delivering better care at lower cost cannot happen without them.

However, if these IT systems lack adequate privacy protections, whether real or perceived, then consumers will likely shy away from providers who have adopted new technology and perhaps not get the care they need or the better quality care that can be delivered with IT.

We need to find the right balance between privacy at all costs and progress at any cost.

Other industries

One approach is to look to outside of healthcare. Healthcare is not the first industry to undergo a shift from paper to modern, electronic tools. (In fact, it is the last.) We can learn how other industries have balanced progress with privacy, from financial services and online banking to online shopping and ATMs. How did these technologies prosper and grow while protecting privacy and security? Certainly there are continuing issues to address, but healthcare can learn from their experiences and adopt what works.

Going back decades, innovators and entrepreneurs have long sought how to protect and secure data while making it portable. In 1984, D.W. Davies and W.L. Price published *Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer*. The publisher noted that the book addressed, "How to use cryptography to protect data in teleprocessing systems--not only keeping data secret but also authenticating it, preventing alteration, and proving its origin."

Today virtually every bank in the United States offers online banking, where we can transfer money from one account to another; pay bills; view statements; and securely communicate with bank representatives. Financial data is not quite as sensitive as personal health information, but it is close. And consumers must still make the decision on whether to use information technology to share, post, and/or store their data online—or to be customers of institutions that do this.

Security and privacy are common concerns among consumers, and there are privacy and security vulnerabilities to address. A recent study found that security flaws in online banking services were widespread, endangering personal financial information.[1] Despite this, Americans increasingly trust and use the technology.

[1] Atul Prakash, University of Michigan, Department of Electrical Engineering and Computer Science, "Analyzing Web sites for user-visible security design flaws." July 2008. http://www.ns.umich.edu/htdocs/releases/story.php?id=6652 (Accessed January 23, 2000).

The Pew Internet & American Life Project reported this month that 55 percent of Americans have used online banking services.[2]

The same can said for e-commerce or online retailing. Credit card fraud, identity theft, and phishing are real threats for consumers that can compromise bank accounts, passwords, and other sensitive data. *The Washington Post* reported last summer that a Russian cyber-crime gang had compromised more than 378,000 computer systems over a sixteen-month period.[3]

Despite the threats e-commerce continues to grow at a remarkable pace. The Census Bureau reported that total e-commerce sales in 2007 were $136 billion, a 19 percent increase from 2006.[4] Online sales now account for 3.4 percent of all retail sales in the U.S., a nearly six-fold increase since 1999.[5]

Consumers know the risks, but they have increasing faith that online services are secure and their financial data is safe. And these services are, for the most part, incredibly secure. Technology programmers from across the globe have worked tirelessly to build secure hardware, software, and networks that protect privacy and sensitive data.

One of the key reasons for success has been technical cooperation throughout the industry to develop common, uniform standards of data transmission. From electronic signatures and security certificates to authentication rules and data encryption, common standards allow for the safe, secure sharing of information that protects privacy. Organizations like the American National Standards Institute (ANSI), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Federal Financial Institutions Examination Council, and the Payment Card Industry Security Standards Council have collaborated to create a common foundation to securely share sensitive information.

The healthcare industry is working with many of these organizations, as well as others, to create common data standards of securely sharing personal health information while protecting privacy.

What is healthcare doing?

Much of the industry collaboration has been done through organizations like Integrating the Healthcare Enterprise (IHE), Health Level Seven (HL7), the

---

[2] Pew Internet & American Life Project, Latest Trends, January 2009. http://www.pewinternet.org/trends/Internet_Activities_Jan_07_2009.htm (Accessed January 23, 2009).
[3] Brian Krebs, "Online Crime Gang Stole Millions," Washingtonpost.com, August 7, 2008. http://voices.washingtonpost.com/securityfix/2008/08/online_crime_gang_stole_millio.html (Accessed January 23, 2009).
[4] U.S. Census Bureau, Quarterly Retail E-commerce Sales 4th Quarter 2007, Released February 15, 2008. http://www.census.gov/mrts/www/data/html/07Q4.html (Accessed January 23, 2009).
[5] Ibid.

CORE initiative of the Council for Affordable Healthcare Quality (CAQH)*, the Healthcare Information Technology Standards Panel (HITSP), and the Certification Commission for Healthcare Information Technology (CCHIT).** The latter two are of particular importance.

HITSP is a cooperative partnership between the public and private sectors, operated under the aegis of ANSI. Its mission is to "harmonize and integrate standards that will meet clinical and business needs for sharing information among organizations and systems."[6] Created through the leadership of former HHS Secretary Mike Leavitt and former National Coordinator for Health Information Technology David Brailer, one of its key priorities has been to develop industry standards on securely sharing personal health information while protecting patient privacy.

Much progress has been made. Through the Security, Privacy & Infrastructure Domain Technical Committee, HITSP has finalized and released a series of industry-wide technical standards that can be incorporated into IT products to secure personal health information and control access to it.

The following selected standards and specifications have been recognized or released—ranging from patient consent directives and access controls to data anonymization and audit trails—and all can secure sensitive information and give patients control over their data.

TP 20 - Access Control Transaction Package

The Access Control Transaction Package provides the mechanism for security authorizations which control the enforcement of security policies including: role-based access control; entity based access control; context based access control; and the execution of consent directives. An example of this is a functional role that has the permission to perform an act (e.g., consumer updating a Personal Health Record (PHR). In an emergency, this construct must support the capability to alter access privileges to the appropriate level (failsafe/emergency access), which may include override of non-emergency consents.

TP 30 - Manage Consent Directives Transaction Package

The Manage Consent Directives Transaction Package describes the messages needed to capture, manage, and communicate rights granted or withheld by a consumer to one or more identified entities in a defined role to access, collect, use or disclose individually identifiable health information (IIHI), and also supports the delegation of the patient's right to consent. The transactions described in this construct are intended to be carried out by HITSP/TP13 - Manage Sharing of Documents.

T 15 - Collect and Communicate Security Audit Trail Transaction

The Collect and Communicate Security Audit Trail Transaction is a means to provide assurance that security policies are being followed or enforced and that risks are being mitigated. This document describes the mechanisms to define and identify security relevant events and the data to be collected and communicated as determined by policy, regulation or risk analysis. It also provides the mechanism to determine the record format to support analytical reports that are needed.

T 17 - Secured Communication Channel Transaction

The Secured Communication Channel Transaction provides the mechanisms to ensure the

---

* CAQH is a member of the Center for Health Transformation.

** Disclosure: I am a member of the Board of Commissioners for CCHIT. However, the views expressed here are mine and do not necessarily represent those of CCHIT.

[6] Health Information Technology Standards Panel, www.hitsp.org. (Accessed January 23, 2009.)

authenticity, integrity, and confidentiality of transmissions, and the mutual trust between communicating parties. Its objectives include providing: mutual node authentication to assure each node of the others' identity; transmission integrity to guard against improper information modification or destruction while in transit; and transmission confidentiality to ensure that information in transit is not disclosed to unauthorized individuals, entities, or processes.

C 19 - Entity Identity Assertion Component

The Entity Identity Assertion Component provides the mechanisms to ensure that an entity is the person or application that claims the identity provided. An example of this Component is the validation and assertion of a consumer logging on to a Personal Health Record (PHR) system.

C 25 - Anonymize Component

The Anonymize Component provides specific instruction for anonymizing data that are prepared for repurposing data created as part of routine clinical care delivery. This construct defines the Component specification that provides the ability to anonymize patient identifiable information.

Source: Health Information Technology Standards Panel

This is real progress on actually delivering security and patient control to ensure privacy. Now that these standards are available, it is up to information technology vendors to implement them in their products. One way to drive this is through the certification process of CCHIT.

The mission of CCHIT is "to accelerate the adoption of robust, interoperable health information technology by creating a credible, efficient certification process." It tests a range of products, including electronic health records, to ensure that products meet a certain level of functionality, interoperability, and security.

According to CCHIT, in its document entitled "CCHIT Certification – What Does It Require?," the certification process requires ambulatory EHR products to provide state-of-the-art technical capabilities needed to keep patient information safe and secure. There are approximately 50 security criteria. To be certified, an EHR must meet 100 percent of these criteria. The broad areas covered include:

- Authentication of users (proving identity);
- Controlling access based on the user role or the context of a care situation;
- Auditing every access and use of a record;
- Encryption of any data sent out of a system;
- Protection against viruses and other malware; and
- Backup of data to prevent loss in case of computer failure or disaster.

Standards identified by HITSP are transferred to CCHIT, where the implementation of those standards in actual products is verified. Every certified electronic health record product must meet these requirements. The information that is captured and stored using certified products is secure, which in turn goes a long way to protecting patient privacy. As HITSP continues to develop and improve security and privacy data standards, they will become additional criteria for certification and, in turn, integrated into the marketplace.

On a general note, policymakers are currently debating the future of HITSP and CCHIT, as well as the National eHealth Collaborative (NeHC), formerly known as

the American Health Information Community. One question under consideration is whether these organizations should continue their work or be replaced or diminished by new organizations. I cannot state in stronger terms that these organizations should continue and that no new organizations should be created.

Some have argued that they have not delivered widespread adoption of health information technology. Several years ago two of the biggest cries were that no entity existed to certify products with a "seal of approval" and that there was no industry-wide movement to develop common data standards. By addressing those concerns, HITSP and CCHIT have indeed contributed to adoption. The single most important missing piece to expedite adoption is realigning provider incentives. Healthcare payers, both public and private, must collaborate with providers to overcome the well-documented financial barriers to adoption.

Others argue that these organizations be replaced because they have not created a finalized, perfected framework of interoperability standards. This is certainly true, in that comprehensive interoperability is not yet a reality, but these organizations have laid far more groundwork in their three to four years of operation than was accomplished in the previous twenty.

Still others argue that the federal government should be a more active leader in driving these processes. One of the key advantages of the current governance is that it truly is a public-private partnership. The federal government is represented and actively participates in HITSP, CCHIT, and NeHC. This balance is necessary. It combines the expertise and market presence of private industry with the purchasing and regulatory power of government.

Replacing these organizations now with new organizations or confusing the marketplace with parallel organizations, requirements, and processes literally turns the clock back four or five years, when the industry first debated this kind of governance. If the existing governance is not given time to work, if we revisit this debate now, the entire industry will pay a huge opportunity cost in time and resources.

To be sure, there are improvements that can be made. HITSP should have firm, aggressive deadlines to complete remaining standards of interoperability, security, privacy, and any new standards that may be proposed. HITSP and CCHIT should formalize the handoff of standards, so that there is a documented process for these standards to become certification criteria. HHS could shorten the length of time of adopting standards. HHS could also fund additional value cases to expedite adoption. The Congress could help as well, by providing incentives as soon as possible—and not waiting until 2011—in addition to requiring that any electronic health record purchased with federal dollars must be CCHIT-certified.

In general, the current structure is working. Security and privacy standards have been developed and released that can secure sensitive information; authorize and

track access; authenticate users; encrypt and anonymize data; and other key priorities.

Proposed legislation

The current governance structure is delivering the technical standards of how to secure data and protect patient privacy, but there are key policy questions that are under consideration that will drive the broader agenda. The House Energy and Commerce committee introduced legislation last week that contains a range of proposals that impact privacy and progress, and members of the United States Senate will soon debate their own proposals.

One of the most controversial issues is patient privacy. Some advocates for very strict privacy protections have outlined specific changes they support. Many in the industry have recoiled at them, as they view many of the proposed requirements as onerous, administrative nightmares. There is a middle ground. There are details to be worked out, but the following proposals include principles and policies that can be balanced to help find consensus.

Individual consent

Yes, there should be a legal framework that includes the right of individual consent. Patient consent can be balanced so that it does not impose new, undue burdens on providers, health plans, and other entities.

One way to accomplish this may be through a uniform patient consent form. Such a form could specify standards and instructions that "clearly reflect patients' rights to information in their medical records and provider confidentiality principles."[7] Such a form could be collected at the time of enrollment in a public or private health plan or before services are delivered. Consumers could opt-out of certain products, services, or notifications and specify how their specific identifiable information can or cannot be shared outside the course of treatment or payment. Some questions will need to be addressed, such as what to do when consent has not been or cannot be given. The Congress should allow the regulatory process to answer such questions.

Another important balance is between identifiable information and de-identified data. We must balance consent and privacy with health services research and public health. I am a strong believer in the power of data. When medical data is turned into secure, actionable knowledge, it saves lives and saves money. Data can reveal which treatments work and those that do not; the effectiveness and relative value of drugs, devices, and medical procedures; variation in the delivery of care; who may be a good candidate for clinical trails; and other vital information that benefits all.

---

[7] RTI International, *Privacy and Security Solutions for Interoperable Health Information Exchange: Assessment of Variation and Analysis of Solutions*, July 2007. http://www.rti.org/pubs/avas_execsumm.pdf (Accessed January 24, 2009.)

It is an indisputable societal benefit to generate this kind of knowledge. It delivers better health at lower cost. But it is simply impossible to do without the wide aggregation and availability of de-identified data. Because the data is de-identified, meaning that all identifiable markers are stripped away that can be traced to a specific individual, personal privacy is protected.

Additionally, there are certain services that health plans offer to their members or that health systems do on behalf of their patients that should still be made available. Disease management, chronic care management tools, and other valuable services should be recognized as treatment and not have new onerous restrictions on identifying possible enrollees or patients who would benefit from a particular medical program.

Data breach notification

Yes, patients should be notified of egregious breaches of privacy and security. We expect our banks, credit card companies, or other financial institutions to do this when our financial data is compromised. So, too, must healthcare organizations.

The standard for what defines a breach must be set very high; as there must be a balance between informing patients and burdensome reporting requirements for health plans, physicians, and other providers.

Protections should incorporate a risk-based notification, so that physicians, health plans, and health systems do not notify patients for harmless or inadvertent data sharing. If, for instance, a physician mistakenly sees the record of a patient he or she is not treating, should that qualify as a data breach? Should the patient whose record was seen be notified? The bar should be set very high so that these types of cases do not generate unnecessarily notifications.

When a notification is required, informing patients must make sense. For instance, does it make any sense that a health plan or provider who lacks updated contact information for patients whose privacy has been breached be required to post on their homepage or take out an ad in a major media outlet that the patient's privacy has been breached? No patient would want that advertised.

Enforcement

Yes, new protections will need to be enforced, and this should be done through existing offices and departments. The last thing our health system needs is more bureaucracy, such as new privacy consultants at HHS regional headquarters or a new office of health information privacy.

Patients should have a private right of action in federal court for extreme breaches of privacy. Again, there must be a balance; this time between patient privacy and creating a new legal market for frivolous lawsuits. To strike the right balance, the bar must be set very high so that federal—not state—litigation is available for patients, but only for clear, egregious cases.

Additional patient protections should be added for deliberate or extreme breaches of privacy. One step in the right direction is to dramatically toughen existing penalties. The Congress should closely examine possible changes to Title 18 of the U.S. Code of Criminal Procedures that would harshly punish the malicious use of personal health information, such as hacking into electronic medical records and publishing or posting online any personal health information. Another option would be to expand current breach-of-privacy laws to include healthcare.

Personal Health Records

Broad-based regulation of personal health records offered by non-covered entities or non-business associates is too early. Patients already have the power to choose whether or not to use such portals and many give patients total control over how their information is shared; who can access it; and if their personal health information can be used to tailor services.

The value of these kinds of products and services is clear. Personal health records and other portals can inform and educate consumers about their health and empower them to better manage their healthcare records that are currently fragmented across the system. Despite these benefits and others, consumer portals are relatively new to the market and still need time to mature. Regulation of any product that is in such a state of infancy will undoubtedly harm their growth—and in this case suffocating the growth of personal health records would rob consumers of their obvious value.

Where changes could be made are to promote "portability" within HIPAA. Consumers should have the legal authority to direct their data to third parties or CCHIT-certified technology products; consumers should have a right to standardized electronic copies of their data with near real-time compliance. These kinds of changes to existing law will not only empower and protect consumers but drive growth in the market. These ideas, as well as bringing stand-alone personal health records under HIPAA, should be studied fully.

Conclusion

We need policy solutions that properly balance privacy with progress and do not go too far in either direction. The risks of favoring one side over the other are real. If privacy protections go too far and place burdens on providers, they will not adopt new technology; and even if they do, valuable data that does not infringe upon privacy could be trapped. However, if privacy protections do not give patients true control over their personal health information or puts that information at risk, we could build the most modern system, and no one would trust it.

We do not need to make a choice between protecting privacy at all costs and making progress at any cost. We can find the right balance if we are careful, judicious, and realistic. Once we do, we will have succeeded in transforming healthcare into a system that saves lives, saves money, and protects privacy.

Appendix I

Excerpted testimony of former Speaker of the House Newt Gingrich

Founder, Center for Health Transformation

House Government Reform Committee

March 15, 2006

The Individual Owns Their Personal Health Record and All of their Health Data

With the rapid development of individual-centered health information technology such as the personal health record, the question then arises, "Who owns the data?" Doctors, hospitals, and other providers often believe that they own the encounter data because they saw the patient and collected the information. Employers and health plans often believe that they own the data because they paid for the services. Laboratory companies, pharmaceutical manufacturers, and other stakeholders often believe they own the data because they ran the tests or provided a product or service to the patient.

All are correct to some extent, but they forget that there is one constant variable running through all these scenarios: the individual. The individual owns the data, which they can then allow each stakeholder to have a copy of their data.

Individuals have the right to control—and must have the ability to control—who can access their personal health information. All health information technology should be deployed to improve individual health, not to protect the status quo of proprietary claims to data. In this case, where federal employees may decide to activate a personal health record, each stakeholder should be given equal access to the record—by the consumer—in the course of delivering care.

###

Appendix II

"Protecting Privacy and Confidentiality in the Nationwide Health Information Network"

By Mark Rothstein

From the book *Paper Kills*

Edited by David Merritt

Published by Center for Health Transformation

CHAPTER 2

Protecting Privacy and Confidentiality in the Nationwide Health Information Network

Mark A. Rothstein, J.D.*

Editor's Introduction

Information about our health and healthcare is by far the most sensitive data we own. From chronic conditions to medications to genetic makeup, our personal health information reveals intimate details about who we are, what we do, and what we may be like in the future. Thus, protecting our privacy and confidentiality is a principle that simply cannot be compromised. As the pace of modernizing healthcare quickens through health information technology, tension grows between protecting patients' personal data and having instant access to their comprehensive medical histories. On the one hand, having real-time access to personal health information—such as current medications and allergies—can often mean the difference between life and death. On the other hand, the release of such sensitive data to outsiders, especially those with nefarious or self-interested intentions, can have disastrous consequences. An interoperable, nationwide system will undoubtedly save lives and save money, and it is an absolutely essential part of transforming health. But it must be built, deployed, and adopted in a manner that ensures responsible, appropriate, and authorized use.

Privacy, including health privacy, is an intriguing concept. In the United States, virtually everyone is in favor of health privacy. But when people are confronted with the costs it entails—in inconvenience and expense—the public's support for it declines. Furthermore, there is no generally accepted definition of what health privacy actually means. For instance, the primary privacy concerns of the public

* Mr. Rothstein serves as Chair of the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics, the federal advisory committee charged with advising the Secretary of Health and Human Services on health information policy. The views expressed in this chapter, however, are solely those of the author.

regarding adoption of electronic health records (EHRs) are that irresponsible healthcare entities and rogue employees will divulge information or that snoops and hackers will get access to private information,[1] but these concerns are more properly characterized as health information security issues.

The definition of health privacy comprises at least the following four meanings: (1) informational privacy, which concerns access to personal information; (2) physical privacy, which concerns access to persons and personal spaces; (3) decisional privacy, which concerns governmental and other third-party interference with personal choices; and (4) proprietary privacy, which concerns the appropriation and ownership of interests in human personality.[2]

Confidentiality is closely related to privacy. It refers to the conditions surrounding a situation when information provided within a confidential relationship (e.g., physician-patient) may be disclosed to others. Confidentiality has been a cardinal principle of medical ethics since the time of Hippocrates. With confidentiality, physicians offer their patients the following arrangement: accept a lower level of control over your sensitive health information (confidentiality vs. nondisclosure), because doing so is important to your health, and your information will not be disclosed without your permission.

Privacy and confidentiality are sometimes viewed as individual rights that clash with the societal interest of disclosure of health information. In fact, society has a strong interest in protecting privacy and confidentiality because public health would be endangered if people were afraid to share sensitive information with their healthcare providers. At the same time, individuals have a strong interest in disclosure, because medical research and other social goods depend on the availability of individual health information. Thus, the costs and benefits of privacy and confidentiality need to be balanced for the benefit of both individuals and society.

The development of the Nationwide Health Information Network (NHIN) raises important questions of privacy and confidentiality. As the amount of easily accessible health information increases, so too do the potential risks to privacy and confidentiality stemming from inappropriate disclosures. Consequently, unless the public is satisfied that adequate measures are in place to protect

health information, the political viability of the NHIN will be threatened.[3]

Today's Protections for Health Privacy and Confidentiality

America's healthcare system protects privacy and confidentiality in three ways. First, confidentiality is a basic element of medical ethics. In 1847, the first Code of Ethics of the American Medical Association (AMA) expressly recognized the importance of confidentiality,[4] and all subsequent versions of the AMA Code, as well as the ethical codes of nurses, dentists, pharmacists, and other health professionals, recognize the importance of confidentiality.[5] Regardless of legal protections or health information technology, confidentiality is, in the first instance, based on the integrity and professional ethics of those who use health information in providing care.

Second, health privacy and confidentiality are protected by a patchwork of federal and state laws. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule[6] is the closest thing to a comprehensive health privacy law, but it has limited coverage. The privacy provisions are part of a federal law addressing health claims, and therefore they apply only to health providers, health plans, and health clearinghouses that submit or pay health claims in standard electronic formats. Thus, HIPAA does not apply to employers, schools, life insurers, and other entities that routinely access, use, and disclose health information. Nor does it apply to the myriad providers who do not submit claims in electronic form. Information protected while under the custody of a covered entity loses its protected status when it is disclosed to a non-covered entity. Furthermore, there are few limits on the re-disclosure of health information to "business associates" of covered entities, including those located off-shore.

Other federal laws have even more limited applicability. For example, the federal Privacy Act[7] applies only to health information in the possession of the federal government. Another law protects the confidentiality of substance abuse treatment information,[8] so that illicit drug users (who are breaking the law) will seek treatment without fear of arrest. The Americans with Disabilities Act limits the types of health record disclosures permissible in the employment setting.[9] Other laws deal with health information in biomedical research.[10]

Several states have laws setting forth privacy and confidentiality rules for healthcare, such as the need for patient consent for disclosure of information.[11] Many states also have laws applicable to certain types of information, such as mental health records, genetic information and HIV/AIDS status. These laws attempt to protect what is perceived to be some of the most sensitive or stigmatizing information.

The third factor protecting the confidentiality of health information is the fragmentation of our largely paper-based health records system. As a practical matter, it would be virtually impossible to identify and aggregate all an individual's medical records, which might be stored in dozens of physicians' offices, hospitals, laboratories, and other facilities in diverse locations. Consequently, individuals can be fairly certain that the otherwise lamentable lack of coordination of their health information has the indirect effect of protecting from disclosure disparate health records that could contain sensitive information. This inadvertent protection, however, is likely to disappear with the creation of the NHIN.

Patients' Rights

A health records system that respects privacy and confidentiality should empower individuals to take an active role in deciding the proper use and disclosure of their health information. To accommodate wide choices for patients, a health record system must be flexible; but if patients have too much control over the content of health records, the records might be inadequate to provide essential information for healthcare. Thus, recognizing the importance of meaningful patient choice over aspects of their health records should not be seen as endorsing unlimited patient control.

The Right to Accept or Decline Participation in the Nationwide Health Information Network (NHIN)

The precise structure and operating mechanism of the NHIN have yet to be determined. Under any likely arrangement, however, individual electronic health records will be accessible via an interoperable network. At the very least, individuals should have the choice whether to make their health records available via the NHIN. It is not entirely clear what such a decision would mean in practical terms. For example, would it still permit the individual to elect, on a

one-time basis, to send a particular set of medical records over the NHIN? If so, then the difference between individuals whose records may be sent "automatically" over the NHIN and those whose records require a special, one-time authorization may be slight. To protect themselves, healthcare providers might require individual authorizations for each non-emergency use of the NHIN for all of their patients. The effect would be to turn all patients into potential one-time users, albeit at a high administrative cost.

The choice to participate in the NHIN is only a starting point. How are such decisions to be made? The most common way of framing the issue is to ask whether the system should be "opt-in" or "opt-out." In the former situation, the presumption or default is that individuals are not part of the NHIN until some express action is taken to permit disclosure. In the latter, individuals could elect not to be a part of the system, but if they do nothing, their records would be accessible via the NHIN.

Although I support the opt-in approach because it is consistent with numerous other aspects of informed consent in healthcare, in practice, there may be little difference between opt-in and opt-out. An analogous debate arose and continues to exist over the HIPAA Privacy Rule. The original proposed rule required that individuals consent to have their protected health information used and disclosed for treatment, payment, and healthcare operations.[12] The final, revised rule withdrew the requirement of consent; instead, it simply mandates that all covered entities provide a notice of privacy practices to individuals, and covered entities with a direct treatment relationship must make a good faith effort to obtain a signed acknowledgment from the individual of receipt of the notice.[13] In practice, patients are usually asked to sign the acknowledgment without any explanation of what it is and often without even receiving the notice. In this environment, replacing the acknowledgment with a consent form would make no difference to most patients, as they would merely be asked to sign a different HIPAA form, with no further explanation.

Based on the unsatisfactory experience with the HIPAA Privacy Rule's approach to notices and acknowledgments, it is imperative that executing an NHIN opt-in or opt-out document be more meaningful. Patients need understandable, culturally appropriate

information about the significance of their choices. Because settings such as a hospital admissions desk and a physician's office reception area are not the best educational environments, broader public education is needed. No such program was ever implemented for the Privacy Rule, and the experience strongly suggests that unless the NHIN contains a substantial educational component, any process whereby patients indicate their decision about participating in it is likely to be deeply flawed.

The Right to Control the Contents of Records Disclosed via the NHIN
Many (or perhaps most) people are not bothered by the release of "routine" elements of their health records. They are only troubled by the prospect of disclosing the most sensitive material. For example, one study at a major medical center involved 100 individuals from each of the following six disease groups: cystic fibrosis, sickle cell disease, diabetes, HIV infection, breast cancer, and colon cancer.[14] When asked whether special privacy protections should be in place for certain medical conditions, they indicated the following conditions as most in need of special protection (in order of need): abortion history, mental health history, HIV/AIDS, genetic test results, drug/alcohol history, and sexually transmitted disease. Assuming that individuals have the right to choose whether to have their records disclosed via the NHIN, if they lack the ability to designate certain information for nondisclosure, then they will simply decline to be part of the NHIN. Thus, some degree of specificity regarding the records to be disclosed is essential to maximize participation in the NHIN.

It may be difficult to determine the appropriate level of patient control over their health records. If patients have too little control, they might decline to have their records accessible via the NHIN; but giving them too much control might not be a good idea, either. For example, if patients had the right to select *any* items in their health records for nondisclosure via the NHIN, then healthcare providers receiving the records would be unsure as to what items could have been removed. To be safe, many providers might obtain a complete medical history for each new patient, thereby eliminating a primary benefit of the NHIN.

One way of giving patients an appropriate degree of control over their information disclosed via the NHIN would be to establish standard information fields that could be selected by patients for

nondisclosure. Such criteria might be based on the age of the information (e.g., items over ten years old), the type of information (e.g., mental health, substance abuse), the type of provider (e.g., psychiatrist), or other bases. If both patients and providers know the rules of disclosure, then privacy could be protected without the need for taking new comprehensive histories. Physicians might inquire, for example, if information from an "optional" field might affect diagnosis or treatment.

One strategy for implementing the approach of selective nondisclosure is the use of "blocking." Patients could designate certain areas of their records to be blocked from disclosure to all or a subset of their healthcare providers. Nevertheless, even if information is blocked, computerized decision support could still scan blocked information to protect patient safety.

If a patient, for example, is taking medication for a psychiatric condition, and the diagnosis and medication are blocked, the decision support would still check for a possible drug interaction between the blocked medication and a new medication under consideration by the physician. If so, then the physician would receive a message about a drug interaction with a blocked prescription. The physician then could prescribe another medication, obtain information from the patient about the blocked medication, or take other steps. Blocking with decision support is likely to improve patient safety over current prescribing practices, wherein patients often get a second prescription without mentioning the first prescription to their physician.

The Right to Control the Contents of Local Health Records

Focusing attention exclusively on health records as they are transmitted via the NHIN is too narrow. For one thing, in the architecture of the NHIN (or some future version of it), any distinctions between "local" records and "network" records may dissipate. Second, patients may not recognize a distinction between the two aspects of their health records. Thus, the question arises as to whether patient controls over health records should apply to local health records and, if so, how should it be done.

I see no reason why patients should not be able to control aspects of their health records regardless of the location or designation of the status of the records. The privacy interests of patients are

the same, and the practicalities are often the same. For example, in a large, integrated health delivery system, the scope of actual or potential disclosures within the system (not using the NHIN) will exceed the disclosures made via the NHIN from a sole provider to another sole provider.

One way to reduce the scope of disclosure is the use of role-based access criteria, under which the level of access of any healthcare provider within a healthcare institution depends on the role and needs of the individual. Thus, treating physicians and nurses would get a higher level of access than billing clerks and food service workers. Role-based access criteria already have been adopted by many large healthcare organizations with EHR systems, and this requirement should be expressly mandated for all healthcare records systems.

An extremely contentious issue involves destruction of sensitive health records. Should individuals have the right to delete certain information from their files? As noted earlier, in a largely paper-based system, individual privacy with regard to old, sensitive health information is protected because the records tend to "disappear" with age—based on patient relocation, provider retirement, storage issues, or similar factors. In an age of electronic health records, nothing will disappear, and the protections of blocking, role-based access, or other measures will not necessarily relieve the anxiety of individuals who know that embarrassing information is in their health records.

Some physicians strongly object to the concept of patients deleting certain aspects of their medical records and assert that doing so would be unethical, illegal, or would jeopardize patient care. All these arguments are related, but none are persuasive. To begin with, medical records are obtained and retained for the benefit of the patient, and laws or professional standards limiting alteration or destruction of records are for the benefit of the patient. The AMA Code of Medical Ethics provides:

> Physicians have an obligation to retain patient records which may reasonably be of value to a patient. . . .Medical considerations are the primary basis for deciding how long to retain medical records. For example, operative notes and chemotherapy records should always be part of the patient's chart. In deciding whether to keep certain parts of the record, an appropriate

> criterion is whether a physician would want the information if he or she were seeing the patient for the first time.[15]

This provision is instructive because it indicates that it is permissible for certain parts of a patient's record to be destroyed, that medical considerations govern how long records information should be kept, and that benefit to the patient is the overriding purpose of maintaining the records.

There are many examples of sensitive health information in medical files with no continued clinical relevance. Here are two examples:

> (1) A 25-year-old woman comes to the emergency department of a local hospital with bruises and minor lacerations as a result of being abused by her boyfriend. She is treated and released. She promptly breaks up with her boyfriend. Twenty years later, she is happily married to another man and has two healthy children. Does her report of abuse at the hands of her old boyfriend need to remain in her file?
>
> (2) A 25-year-old graduate student celebrates the end of exams with an evening of excessive drinking and carousing, which ends with a liaison with a commercial sex worker. A week later, concerned about the health implications of the adventure, he has his physician run a battery of tests for sexually transmitted diseases. All the tests are negative and the carousing is not repeated. Does the record of sexually transmitted disease testing, and the reason for it, need to remain in his file for the rest of his life?

I would argue that deleting sensitive health information under some appropriate standards and procedures would be ethical, not jeopardize patient health, and would support public health by not discouraging individuals from seeking care in sensitive situations. To the extent that removing certain information is unlawful, which the AMA asserts is not usually the case,[16] applicable laws should be amended or repealed.

The Right to Know Disclosures Beyond Healthcare

The loss of health privacy creates a substantial risk of tangible harm to individuals. Ironically, the disclosures leading to these harms are almost always lawful. In the United States, laws to protect health

privacy are designed to protect against unauthorized access to, use of, and disclosure of personal health information. Few laws place any restrictions on the scope of information that third parties may require individuals to disclose pursuant to an authorization. Individuals need not sign an authorization to release their health records, but if they refuse, they will not be considered for employment, life insurance, or other essential transactions or opportunities. Furthermore, disclosures of health records pursuant to an authorization tend to comprise the entire record, regardless of any limitations listed in the authorization.

Few people realize the pervasiveness of compelled authorizations. In a recent article, Meghan Talbott and I estimated the number of compelled authorizations each year in the United States at 25 million.[17] The list of uses includes health information disclosed for employment entrance examinations, individual health insurance applications, individual life insurance applications, individual long-term care insurance applications, individual disability insurance applications, individual and group disability insurance claims, automobile insurance personal injury claims, Social Security Disability Insurance applications, workers' compensation claims, veterans' disability claims, and personal injury lawsuits. It is impossible to protect health privacy and confidentiality without regulating compelled disclosures of health information.

Although it is often necessary for third parties to consider an individual's health information in each of the uses described above, it is rarely necessary to consider an individual's entire health record. Moreover, with the advent of the NHIN, the amount of information accessible about each individual will increase dramatically. Thus, it is likely that more sensitive health information of no relevance to a non-healthcare use might be routinely disclosed millions of times each year.

Contextual access criteria are computer software programs or algorithms that enable the holders of health information to limit the scope of the disclosures.[18] For example, using this technique, life insurance companies would receive only information related to mortality risk and employers would receive only information related to the individual's ability to perform a specific job. It will be a challenge to develop the criteria for each of the common, non-medical uses of

health information and then to develop the programs to isolate these data fields in electronic health records. It will also be a challenge to garner the political support to restrict the scope of disclosures. Nevertheless, research efforts to develop the technology of contextual access criteria must be undertaken immediately. If the NHIN goes forward without the architecture to support contextual access criteria, it may be impossible or prohibitively expensive to add this feature later.

Nonclinical Uses of the NHIN

A network of interoperable, longitudinal, comprehensive EHRs has many potential applications beyond promoting efficient, effective, and safe clinical care for individuals. The data derived from aggregation of individual health information would provide a rich resource for epidemiology, outcomes research, population health statistics, health quality research, healthcare utilization review, and fraud investigation. Currently, the most aggressive non-clinical use of the NHIN being developed is for real-time biosurveillance, involving natural (e.g., influenza) and man-made (e.g., bioterrorism) health threats.

Although national security is an area of great public concern, using biosurveillance as a prominent initial application of the NHIN raises significant issues. Even if privacy and confidentiality were well protected in a biosurveillance system, an emphasis on this issue might lead members of the public to question the veracity of official pronouncements that the NHIN is being created primarily to improve personal health. Before establishing a national biosurveillance system using the NHIN, five considerations need to be addressed and satisfactorily resolved.

First, public officials need to make a compelling case regarding both the need for and efficacy of such a new system. Pilot projects and smaller start-up measures should be undertaken before the NHIN is used.

Second, the measures used by the system should be the least intrusive possible. The minimum amount of data should be released to the fewest number of people in the least identifiable form.

Third, there should be transparency in establishing the system,

and all stakeholders (e.g., state and local public health officials, healthcare providers, members of the public) should have an opportunity to participate in its design. To date, there has been little notice and even less public participation.

Fourth, public and professional education about the objectives, operations, and safeguards of the system is essential.

Fifth, there should be an ongoing program of independent oversight, assessment, and research to ascertain whether the system is meeting its goals and adequately protecting privacy and confidentiality.

Conclusion

The NHIN is different from other large health database projects because it is intended to facilitate the dissemination of clinical data. The participants in the NHIN are not volunteer research subjects. They are patients in clinical settings who have done nothing to enroll in the NHIN except to enter the healthcare system.

Given this framework, it is clear that the developers of the NHIN have a substantial ethical responsibility not to harm the interests of patients, and to protect their privacy and confidentiality. The interests of patients must take precedence over other intended uses of the system. There must be public participation in the system's design and a well-financed, vigorous public education program before the NHIN goes into effect. Fair information practices, such as accounting for disclosures and a complaint resolution process, should be incorporated into the NHIN. Individuals should have the right to choose whether to participate and, if they do, they should have some control over the content of the health information disclosed. Contextual access criteria to limit the scope of information disclosed to third parties for non-medical purposes should be part of the architecture of the NHIN. Strong enforcement is needed and there should be an ongoing program of research to assess the effects of the NHIN and its privacy measures.

If the preceding list seems long, difficult, and expensive—it is. Privacy and confidentiality are not cheap, and they are not easy. These protections, however, are crucial in establishing and maintaining public trust in the NHIN and its component parts. To do less

would risk losing public confidence in the entire healthcare system and exposing individuals to a range of tangible and intangible harms.

Mark A. Rothstein, J.D., holds the Herbert F. Boehl Chair of Law and Medicine and is Director of the Institute for Bioethics, Health Policy, and Law at the University of Louisville School of Medicine. Professor Rothstein is a leading authority on the ethical, legal, and social implications of genetics, privacy, occupational health, employment law, and public health law. He is Chair of the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics, the statutory advisory committee to the Secretary of Health and Human Services on health information policy, including the privacy regulations of the Health Insurance Portability and Accountability Act. He is the immediate past President of the American Society of Law, Medicine and Ethics. He is the author or editor of 19 books. His latest book is entitled *Genetics: Ethics, Law and Policy.* He received his B.A. from the University of Pittsburgh and his J.D. from Georgetown University.

[1] Harris Interactive, "Health Information Privacy (HIPAA) Notices Have Improved Public's Confidence That Their Medical Information Is Being Handled Properly," news release, February 24, 2005. Available at http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=893 (accessed March 30, 2007).

[2] Anita L. Allen, "Genetic Privacy: Emerging Concepts and Values," in *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era,* ed. Mark A. Rothstein (New Haven, CT: Yale University Press, 1997), 31–59.

[3] National Committee on Vital and Health Statistics, Letter to Health and Human Services Secretary Mike Leavitt, June 26, 2006. Available at http://www.ncvhs.hhs.gov/060622lt.htm (accessed March 23, 2007).

[4] American Medical Association, *Code of Medical Ethics of the American Medical Association,* art. I, § 2, 93 (1847). Available at http://www.ama-assn.org/ama/upload/mm/369/1847code.pdf (accessed March 30, 2007).

[5] Rena A. Gorlin, ed., *Codes of Professional Responsibility: Standards in Business, Health and Law,* 4th ed. (Washington, D.C.: BNA Books, 1999).

[6] 45 C.F.R. Parts 160, 164 (2004).

[7] 5 U.S.C. § 552a (2000).

[8] 42 C.F.R. Part 2 (2004).

[9] 42 U.S.C. § 12112(d) (2000).

[10] 45 C.F.R. Part 46 (2004).

[11] Joy Pritts et al., *The State of Health Policy: A Survey of State Health Privacy Statutes, 2nd ed.* (Washington, D.C.: Georgetown University Press, 2002). Available at

http://hpi.georgetown.edu/privacy/pdfs/statereport1.pdf (accessed March 30, 2007).
[12] Department of Health and Human Services, "Standards for Privacy of Individually Identifiable Health Information," *Federal Register* 65, no. 250 (December 28, 2000): 82,462-829 (proposed section 164.506(a)).
[13] 45 C.F.R. § 164.520 (c)(2)(ii).
[14] Laura Plantinga et al., "Disclosure, Confidentiality, and Families: Experiences and Attitudes of Those With Genetic versus Nongenetic Medical Conditions," *American Journal of Medical Genetics* 119C, no. 1 (2003): 51.
[15] American Medical Association, Code of Medical Ethics § 7.05: Retention of Medical Records (2006–2007 ed.) (2006).
[16] Ibid.
[17] Mark A. Rothstein and Meghan K. Talbott, "Compelled Authorizations for Disclosures of Health Records: Magnitude and Implications," *American Journal of Bioethics 7*, no. 3 (2007): 38–45.
[18] Mark A. Rothstein and Meghan K. Talbott, "Compelled Disclosures of Health Information: Protecting against the Greatest Potential Threat to Privacy," *Journal of the American Medical Association* 295 (2006): 2882–85.