COMMENTARY

Designing Solutions for Securing Patient Privacy—Meeting the Demands of Health Care in the 21st Century

Benjamin M. Bluml and Glenna M. Crooks

Objectives: To define the issues surrounding patient privacy, examine the political context in which debate is taking place, and present a novel technology model for addressing privacy, confidentiality, and security in 21st century health care. ***Summary:*** The discussion of privacy addresses one of the basic issues in health care today—the tension between the needs of the individual patient for privacy and confidentiality and the needs of society to effectively manage health care practices and control health care costs. Patient concerns for privacy, confidentiality, and security are legitimate, and can usually be reduced to issues that potentially affect an individual's employment, ability to get and maintain health coverage, and have control over his or her records and care. These concerns, combined with several precipitating events, are forcing the issue of privacy into the political arena, where new health policy decisions will be made. The debate must be framed within a principle-centered approach that focuses on boundaries, security, consumer control, accountability, and public responsibility. A global, distributed electronic health record management model that provides location-independent, secured, authenticated access to relevant patient care records by qualified health care professionals on a need-to-know basis provides solutions. Information asset considerations should be designed to equitably represent the ownership needs of corporate entities, society, and the individual. ***Conclusion:*** A secure electronic health record structure that systematically ensures a high level of accountability combined with thoughtful dialogue among key stakeholders in the public policy development process can offer the privacy outcomes we seek.

J Am Pharm Assoc. 1999;39:402–7.

Two trends in health care are moving quickly and with equal force. The health care community, driven by a need to control costs and quality, is developing and using data-rich repositories of health and personal information from patients. Patients, driven by concerns for privacy, are increasingly hostile to the notion that medical information will leak outside of health care providers to employers, insurance companies, and law enforcement agencies.

In the current dialogue between the health care and patient communities, the two forces often appear diametrically opposed, and while the conflict is likely to become increasingly intense, that need not be the case. We believe that there are solutions that can meet everyone's needs. To find those answers, all of the parties involved should pause, take a step back from the brink, and expand the discussion to include solutions, not just fears.

For health care providers concerned about increasing expenditures, this means stepping back from the fear that not having access to complete patient data will cripple management and retrospective research. For consumers alarmed by stories of big government and big business having womb-to-tomb access to our most closely held information, "stepping back from the brink" means distancing oneself sufficiently from fears of loss of control and autonomy. Some of these fears may be legitimate, but dwelling on them will preclude an inclusive and rational discussion of the issues. Stepping back will create a calmer climate for discussion and allow both sides to see that many of their values, goals, and objectives are the same. Stepping back will allow cooler heads to prevail as we approach one of the more contentious issues of the early 21st century. What appear to be opposing goals—data acquisition and use versus privacy and confidentiality—need not be. It is incumbent on those who make policy and collect and use data to resolve the conflicts and find the solutions that meet everybody's needs.

For those of us in health care, this impending debate means that, without further delay, we must make every effort to restore and sustain the trust we have so long enjoyed from our patients. We must exercise even greater care to preserve the integrity and

Received March 16, 1999, and in revised form March 31, 1999. Accepted for publication March 31, 1999.

Benjamin M. Bluml is senior director for research, American Pharmaceutical Association Foundation, Washington, D.C. Glenna M. Crooks, PhD, is president, Strategic Health Policy International, Inc., Fort Washington, Pa.

Correspondence: Benjamin M. Bluml, 2215 Constitution Avenue, NW, Washington, DC 20037-2985. Fax: (202) 429-6300. E-mail: bmb@mail.aphanet.org.

confidentiality of the information that we collect, store, and use. We must demonstrate to the public through responsible handling of patient information that the people we are and the systems we operate are worthy of the respect we have been afforded in the past. Acting wisely in matters related to information will protect the rights of patients and prevent the breaches of privacy, confidentiality, and security that incite public ire and drive legislation that could hamstring essential elements of health care services and research in the future.

In practice, the technology already exists to guard patient interests while providing the industry with the information it needs to improve patient care and control costs. An appropriately designed technology infrastructure can meet everyone's goals. Any dialogue needs to take into account the values of both groups. It must incorporate patients' expectations for health care providers, not only in providing care, but in respecting patients' privacy and confidentiality (in short, their dignity). It must incorporate providers' expectations for access to information that will facilitate the research, patient care, and management missions of health care.

In this article we define the issues surrounding patient privacy, examine the political context in which debate is taking place, and present a novel technology model for achieving the expressed goals while offering ways for the health care industry to protect its interests during the current discussion.

Privacy, Confidentiality, and Security

The terms privacy, confidentiality, and security are often used interchangeably. But they are not the same, and an understanding of the differences is important to the ongoing dialogue.

- *Privacy* is the right of the patient that information be kept secret and not shared with any other person. Privacy is based on the notion that the individual has control over personal information. As a result, the individual has a right, under privacy, to decline to have a medical test performed. For example, a woman receiving prenatal care regularly submits blood and urine samples for the purpose of monitoring the course of her pregnancy. The right to privacy dictates that those samples may not be used for purposes unknown to her or without her consent—for example, for HIV or drug use testing, or for the determination of the risks of genetic conditions.
- *Confidentiality* is the protection of that private information, once it is disclosed by the patient, from being shared with others within or outside of health care settings not directly involved in the patient's care. Confidentiality restricts who can see and use that information. As a result, individuals can be assured that sensitive information will not be used for some purpose unknown to them. In the case of the pregnant woman, once she has consented to genetic or HIV tests, then confidentiality dictates that the results of those tests will not be disclosed to others outside the arena of her health care—for example, to insurance companies, state disability agencies, or product marketing firms.
- *Security* is achieved by the policy, procedures, and technologies that prevent the disclosure of confidential or sensitive information, and by extension, the harmful effects of that disclosure. Security involves both the human and the technical aspects of protecting information. Again, for example, the pregnant woman expects that the sensitive information collected about her will be handled carefully by each person who accesses it, and that records will be transmitted and stored securely.

Real Issues and Real Concerns

Patients' concerns for privacy, confidentiality, and security are legitimate. At the core of it, patients need and want to protect privacy and assure the confidentiality of medical information for two reasons: (1) it is their right to do so; and (2) inappropriate disclosure of medical information can create serious problems in their lives. Health information can be used to affect or deny employment or health coverage. The revelation of some types of sensitive information, such as a genetic predisposition to disease, history of mental illness, HIV infection, or history of substance abuse, can seriously compromise a patient personally, professionally, and financially. Disclosure of such information to insurance companies, managed care companies, or law enforcement agencies could result in discrimination or harassment.

A true patient-centered health care information system will take a dual approach: recognizing the rights of the patient while managing information through the best policies and procedures our systems can offer. This dual approach will be supported by an ongoing dialogue between health care providers and consumers and facilitated by increasingly sophisticated information technology.

Today's Policy and Politics

As we move toward the 2000 presidential campaign, health care is certain to be one of the issues in the political debates ahead. External precipitating events may force Congress and the administration, however reluctantly, to tackle the issue of privacy. Some of these events have already occurred:

- The European Commission, through its Privacy Directive, does not allow member states to transfer any data, including health care data, to any other country unless the recipient country has adequate privacy controls. The U.S. Department of Commerce suggests that American industries can self-police through voluntary internal guidelines, but this U.S. response has been criticized as inadequate. Although past the deadline for implementation, the European Commission has not yet enforced this directive. It is likely that the Commission will enforce the directive at some point, and the U.S. response will again be scrutinized.

- The Health Insurance Portability and Accountability Act of 1996 (also known as Kennedy–Kassebaum) requires that Congress pass privacy legislation by August 1999. If it fails to do so, the Secretary of the Department of Health and Human Services must impose regulations on privacy by February 2000. Knowledgeable observers believe both deadlines will slip, partially in deference to Y2K issues.
- A series of hearings scheduled last summer to discuss unique health identification numbers for American citizens ended abruptly when a public outcry erupted. Improving health care did not stand up well against fears of "Big Brother" data-gathering conspiracies voiced by consumer advocates. Editorials from coast to coast warned of "womb-to-tomb" privacy invasions enabled by the unique numbers.
- A widely publicized story that originated in the *Washington Post* in February 1998 erroneously suggested that CVS and Giant pharmacies had sold customer lists to Glaxo Wellcome to market directly to patients. Following the publicity and customer complaints, CVS canceled its compliance program and Giant halted one it had planned. Within days, a customer had filed a class action suit against the pharmacies, Glaxo Wellcome, and the compliance program business (Elensys, Inc.) that had sent the letters. The suit has been expanded to include Warner-Lambert, Merck & Co., and Hoffmann-LaRoche.

The 105th Congress saw three bills in the Senate and one in the House of Representatives that directly addressed patient privacy. Attempts at tackling the issue are worth reviewing, because they presage some key elements that future legislation will likely address, in particular the degree of patient consent required for data access, the protection of data for research, and the federal preemption (or "override") of state law. Several pieces of legislation reintroduced in the 106th Congress that directly address patient privacy, while not available for review when this article was written, reportedly are similar to the bills introduced in the last Congress.

In the 105th Congress, Sen. James Jeffords (R-Vt.) and Sen. Christopher Dodd (D-Conn.) introduced the Health Care PIN Act (S.1921), which required patient consent authorizations for release of information for any purpose other than treatment, payment, or health care operations. This bill preempted weaker, less protective state laws, but allowed stronger, more protective state laws to stand. Sen. Patrick Leahy (D-Vt.) introduced the Medical Information Privacy and Security Act (S.1368), which allowed patients to designate which entities would not receive confidential information. A proposal (never formally introduced) by Sen. Robert Bennett (R-Utah) was similar to the popular Jeffords version, but would have preempted all state laws. The House bill (HR 3900) introduced by Rep. Chris Shays (R-Conn.), titled the Consumer Health and Research Technology (CHART) Protection Act, protected information for research by allowing data to flow to specifically designated projects without patient consent and preempted state laws except for public health purposes.

In 1998 at least 250 bills addressing patient privacy were introduced in the states. That activity is not likely to abate soon, as some of the recently proposed federal legislation opens a brief window during which states can enact their own laws before preemption begins.

Framing the Debates

As policy is debated and legislation is introduced, a set of principles and practicalities will likely frame the discussion. The principles were developed by Secretary of Health and Human Services Donna Shalala[a] and issued in her recommendations to the National Committee on Vital and Health Statistics (which is studying health information issues under mandate from the Health Insurance Portability and Accountability Act of 1996). The practicalities are the program realities that must be considered as legislation and regulations are written concerning the collection, use, and management of data.

The Secretary's five principles are:

- *Boundaries.* Health care information should be used for health purposes only, subject to a few carefully defined exceptions.
- *Security.* Organizations entrusted with health care information should protect it against deliberate or inadvertent misuse or disclosure.
- *Consumer control.* Patients should have the right to view and correct records, obtain copies, and know who has accessed them.
- *Accountability.* Those who misuse personal health information should be punished.
- *Public responsibility.* Individual claims to privacy should be balanced with the public good.

The practicalities involved in applying these principles include:[1]

- *Data collection and use.* What data will be collected, and how will it be used? What identifiers will be used? Must patients consent to the use of their medical records in health outcomes research? Should law enforcement officials be allowed access to records? Will pharmacies be prevented from using information contained in their databases to monitor compliance?
- *Data management.* How will data be managed to preserve privacy, confidentiality, and security? Does a patient have a right to privacy on all medical matters, including communicable diseases? Once a patient discloses private information, how long must confidentiality be maintained? Should those using confidential information be subject to criminal background checks? Should data disclosure be required as a condition for receiving health insurance coverage?
- *Patient rights to view and correct records.* What rights will patients have to view and correct medical records? Who will prevail if a patient and a physician disagree on information in the record? How will patients be allowed access to records? If uncorrected records are shared and the patient later learns of inaccuracies, must the corrections be shared with all prior users?
- *Limits of consent and authorization.* Should consent be required for each use of the patient's data? Should patients be reimbursed for the use of the data? Should patients be required to opt in or out of pharmacy monitoring and compliance programs?

- *Penalties.* How will intentional and unintentional violations be punished? Are individuals as well as corporations responsible for violations? Should data managers and repositories be licensed? Will pharmacists (as individuals) or the pharmacy be held responsible for the confidentiality of patient records?
- *Federal preemption of state laws.* Will federal laws preempt state laws? Should federal laws create a "floor" over which stricter state laws can be imposed? How will conflicts between state insurance laws and federal privacy laws be resolved?

The Distributed Electronic Health Record Management Model

Health care delivery is complex, with many different needs depending on the system in question, and it would be difficult—if not impossible—to establish a design for every conceivable situation. We think that models can be helpful for structuring the elements of solutions, however, and we propose one here (Figure 1). The Distributed Electronic Health Record Management Model describes critical elements in technology and provides a framework for assessing what information is collected and shared, by whom, for what purpose, and at what level of accountability. As discussed below, this model comprises four components: the electronic health record, health information service providers, health information authorities, and users.

Component 1: Electronic Health Record

The electronic health record (EHR) is envisioned as a global, distributed structure-and-process model that contains four distinct information "silos": personally identifiable data, claims transaction data, clinical encounter data, and quality event data. Each record in these silos contains an encrypted, anonymous patient identifier. In addition, an accounting layer houses two specific record stores: audit trails and transaction histories.

Key examples of specific elements contained within each silo can be found in a variety of existing work from the American National Standards Institute Healthcare Informatics Standards Board, the American Society for Testing and Materials health care informatics standards, the American Standards Committee X12 standards, Health Level 7 standards, the International Electronic and Electrical Engineers technical committees, and the National Council for Prescription Drug Programs (NCPDP) standards, in addition to those from various government and international organizations.

The silo that contains personally identifiable data will contain administrative data, demographic information, legal agreements, financial information, and provider data. It will be accessible by patients, payers, providers, and others as authorized by patient agreements.

The silo that contains claims transaction data will include elements required on such claim forms as the UB-92 and the HCFA-1500, along with other market-specific business transaction data sets such as those from NCPDP. The requisite diagnostic and procedure classification codes, such as the International Classification for Diseases and Current Procedural Terminology, will also be included. It will be accessible by patients, payers, providers, researchers, and others as authorized by patient agreements.

The silo that contains clinical data will include patient history and assessment data, immunization histories, hazardous stressor exposures, problem lists, diagnostic tests, clinical orders, medications, scheduled appointments, and encounter data. It will be accessible by patients, providers, and researchers and others as authorized by patient agreements.

The silo containing quality event data is essential to continuous quality improvement efforts in the health care delivery system. As currently provided for by most state laws, this information will remain legally undiscoverable. It will include events that relate to adverse reactions, clinical interventions, therapeutic evaluation, system errors, and other organizationally defined quality improvement activities. It will be accessible to providers within their employment entities and others as authorized by organizational agreements.

The accounting layer provides features that include reviewable audit trails that track access to records and transaction histories that provide for the re-creation of views at specific points in time. This accounting layer systematically insists on a high level of individual and process accountability for interaction with the EHR.

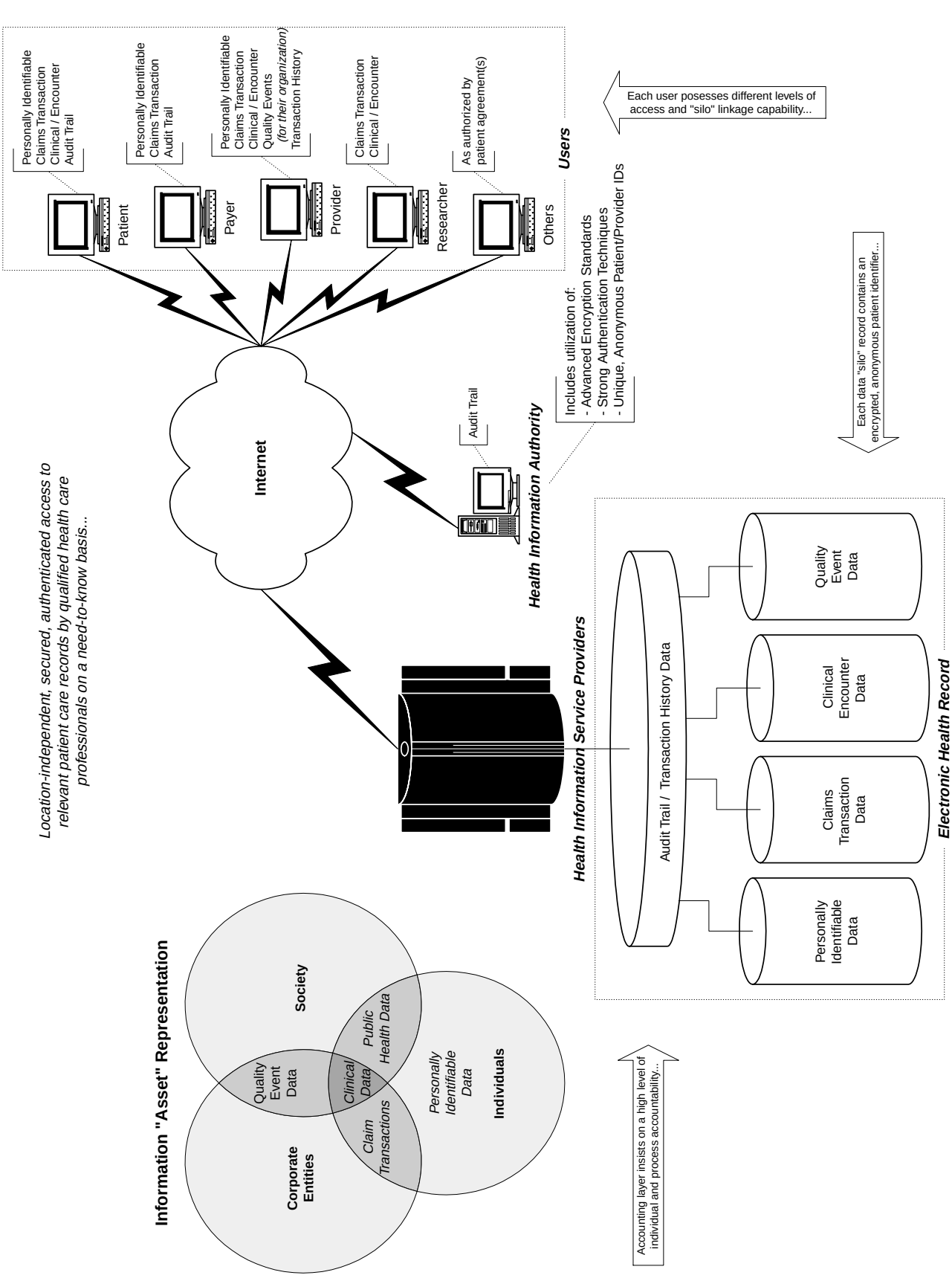
Component 2: Health Information Service Providers

The Health Information Service Provider (HISP) will be responsible for the technical measures required to ensure that data is appropriately stored and secured and continuously available. Health data should be stored within the structure of the distributed EHR management model, and physically secured with redundant real-time, fail-safe system contingencies to ensure referential integrity and availability. Access to information must be guided by the policies and procedures defined by the Health Information Authorities. Authentication of all users, their defined access levels, status according to current records, and record linkage operations should be systematically monitored to ensure appropriate use, with any breaches reported to the Health Information Authorities.

Component 3: Health Information Authorities

Health Information Authorities will be responsible for establishing EHR access policies and procedures and for HISP monitoring to ensure compliance. The Authority will also be responsible for establishing processes that assign unique, anonymous patient and provider identifiers. Prevention, identification, and resolution of internal and external threats should be effectively addressed by the Authority. Ongoing evaluation and monitoring of available technologies for continuously improving authentication and encryption mechanisms will be essential to the long-term success of the system.

Figure 1. A Macro-Level Model for Global, Distributed Electronic Health Record Management



Component 4: Users

Users will fall into several distinct categories—patients, payers, providers, researchers, and others—all possessing different levels of access and EHR silo linkage capability. Levels of access will be tailored to empower the patient, while protecting his or her privacy and creating health care delivery and design efficiencies.

Patients will be able to view their current information at any given point in time. They will have access to and the authority to view records either individually or in a linked fashion between and among the EHR silos that contain personally identifiable data, claims transaction data, clinical/encounter data, and audit trail data. In addition to their viewing privileges, they will have the ability to contribute information to selected portions of the EHR in collaboration with their health care provider(s). They will also have the ability to submit requests for factual corrections to the Health Information Authority in a secure way.

Payers, as authorized agents of the patient, will have access to and the authority to view records either individually or in a linked fashion between and among the EHR silos that contain personally identifiable data, claims transaction data, and audit trail data. In addition, they will have the ability to contribute compensation and reimbursement information to the claims transaction data silo, and will be responsible for notifying the patient of any unauthorized audit trail records identified in their account.

Providers will be designated within patient relationships and authorized accordingly. They will have access to and the authority to view and modify records either individually or in a linked fashion between and among the four EHR data silos. The quality event views will be limited to their organizational affiliation. They will also have the ability to view the EHR in "historical mode" to allow for the "reconstruction" of views that were available at specific points in time.

Researchers will have access to large groups of patient records within Investigational Review Board authorizations. They will not have access to any personally identifiable information, but will have the ability to view records either individually or in a linked fashion between and among the EHR silos that contain claims transaction data and clinical data. This will provide them with the opportunity to conduct clinical, economic, and epidemiologic research using the EHR data without ever knowing the identity of the patients yet having the capability to uniquely identify study subjects across a wide spectrum of care.

Other users will be provided with access through legal agreements with the patient, as consistent with Health Information Authority policies and procedures.

Information "Asset" Considerations

The distributed EHR management model, a limited access interactive communications model for sharing health information, can also be considered according to its fundamental relationships with regard to business entities and the needs of society versus the needs of the individual (see Information "Asset" Representation in Figure 1).

While corporate entities will certainly collect other data (with patient consent) that remain within their domain, and social registries for communicable diseases and public health will also be required, this asset representation tips the balance of ownership toward the patient. Equity and respect for the individual will result in patients who are more informed, involved, and ultimately empowered to be in control of their own health.

A key tenet in any distributed EHR management model must be a stipulation to prevent reverse engineering outside of a priori agreements about specific uses of data. Preventing users from reassembling data from various sources for a use other than that originally specified will result in the preservation of the model's integrity and the public trust essential to the viability of distributed EHR management.

The distributed EHR management model represents a technological solution to a policy and business dilemma. While the dynamic nature of technology and the shifting political winds may make it difficult to keep the model in focus, our commitment to its use over time will result in the generation of new knowledge that fosters continuous system and health care improvements.

Conclusion

We offer this model for discussion in the policy and technology forums of health care. We also offer optimism that the various interests can be reconciled. Continuity and quality of care is jeopardized in the current paper-based medical record system, and security is by no means guaranteed. An electronic environment offers us the opportunity to create better security measures for the important information necessary in a sophisticated health care system. The public policy environment offers us the venue for arriving at the solutions to our concerns about the appropriate use of that information.

Health care providers possess the requisite technological knowledge to take control of the agenda and design practical solutions to the problems. If we do not, the agenda and the solutions are likely to be created elsewhere, with little recognition of the costs and implications for our clinical and economic realities.

[a]Confidentiality of Individually-Identifiable Health Information, recommendation of the Secretary of Health and Human Services, pursuant to section 264 of the Health Insurance Portability and Accountability Act of 1996, Submitted to: The Committee on Labor and Human Resources and the Committee on Finance of the Senate, the Committee on Commerce and the Committee on Ways and Means of the House of Representatives, September 11, 1997.

Reference

1. NWDA Healthcare Foundation. *Examining the Social, Technical and Market Issues Affecting the Confidentiality and Security of Patient Records. The Report.* 1998;1–78.