Balancing Good Intentions: Protecting the Privacy of Electronic Health Information

Kitty McClanahan
University of Tennessee

Electronic information is a vital but complex component in the modern health care system, fueling ongoing efforts to develop a universal electronic health record infrastructure. This innovation creates a substantial tension between two desirable values: the increased quality and utility of patient medical records and the protection of the privacy of the information they contain. This article discusses related U.S. legislation, policy, and law—including the Health Insurance Portability and Accountability Act of 1996. This article offers an inclusive, equilibrium model to conceptualize the spectrum of challenge that this interplay of desirable but oppositional values creates. The model illustrates the relationship between information privacy and information flow, and that between individual and society-level needs, within the resulting impact sectors of individual security, health care priorities, public health effectiveness, and e-health development, while specifying beneficial outcomes for each.

Keywords: *electronic medical record; universal health record; information privacy; HIPAA*

Medical record keeping has historically been a paper-based activity, but since the advent of computerization, the practice has gradually but inexorably involved a migration to electronic record systems (Roach & Aspen Health Law and Compliance Center, 1998). The increased use of electronic medical records has created a substantial tension between two desirable values: the increased quality and utility of patient medical records and the protection of the privacy of the information they contain (Dennis, 2000). In light of this conflict, this article discusses the question of how well existing legislation and policy address the need for privacy protection and their impact on the quality of patient care.

The discussion focuses on the relevant sections of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, 1996), widely recognized as the most significant regulatory action regarding the use and privacy of electronic medical records. Major case law pertaining to the protection of the privacy of patients' electronic medical records is also considered. To assist in informing the dialog on this issue, this article offers a model to represent the tension between privacy protection and information access and the conflict between the needs of an individual patient and the health concerns of society at large. It is anticipated that efforts to resolve these issues may benefit from a greater awareness of the variety of perspectives to be considered in the design and implementation of any solution.

Before addressing the privacy concepts, it is helpful to set the stage by exploring the important role that information management and technology play in the delivery of health care in the United States and current efforts underway to further expand it.

The Information Imperative in Health Care

Information is a vital but complex component in the modern health care system. At a minimum, health care providers need to know a patient's identity and demographic characteristics, recent and distant medical history, current medications, allergies and sensitivities, chronic conditions, contact information, and legal preferences. The longstanding standard practice depends on the patient to supply this information at

AUTHOR'S NOTE: The author is grateful for the helpful comments of Professor Dwight L. Teeter, Jr., PhD, and for the legal research assistance of Jean E. Moore, reference librarian, both of the University of Tennessee.

Bulletin of Science, Technology & Society Vol. 28, No. 1, February 2008, 69-79
DOI: 10.1177/0270467607311485

each point of provider contact in a health care system, with its accuracy verifiable (but not always actually verified) by archived information contained in a static paper or electronic medical record. However, in many situations, the patient or his or her representative is unable or unwilling to provide complete information, and the health care provider must take action based on only partial or even inaccurate information.

In the emergency room in particular, the patient is often unconscious or so ill as to be unable to provide any oral information at all. In such settings, where providers must act quickly, it is much too likely that treatment causing a medication conflict, or ignoring an unexpected underlying condition, could result in harm to or even the death of the patient. In 1999, the National Academy of Science estimated that the annual number of deaths in U.S. hospitals from medical errors was between 44,000 and 98,000, frightening figures that likely substantially underreport the problem (Institute of Medicine, 1999).

If privacy violations were not a problem and quality of patient care were the only objective to be considered, patients would not have to be harmed by or die from an acute shortage of *information*. Advances in networked information technology (IT) make it possible for each person to have a universal electronic medical record, containing his or her complete and always up-to-date medical information. In this situation, the emergency room doctor would instantly know that the unconscious accident victim the paramedics just brought in had a troubling cardiac stress test the day before, is deathly allergic to penicillin, and just started taking a new brand of insulin last week. The doctor would know all of this instantly, because he or she scanned the tiny microchip implanted in the patient's body to retrieve a universal medical unique identifier number, which a nurse then used to access the Universal Medical Database and call up the patient's comprehensive record. Or, in a less invasive solution, the nurse might have found, on the victim's key ring, the small USB digital storage device containing the patient's up-to-date universal health record (UHR). A hospital information specialist would then plug the device into an ordinary computer in the emergency room, access the UHR, and be immediately able to search through the multimedia document, using whatever search terms the doctor requested, based on a physical appraisal of the patient's condition.

The UHR

The above-described scenario is not a vision made of science fiction; it is actually based on technology available now that could be implemented through procedural systems that are currently in development. Microchip implants are widely used to identify pets and to track livestock (DeMoss, 2006) and could also function well in human beings, if they become socially acceptable.[1] The less-intimidating USB keychain (or necklace) device is called a Personal HealthKey and is manufactured by the CapMed Company. Consumers can order it online for less than $100.[2] The HealthKey contains all the software necessary to display and access the health record from any PC, and it interfaces with many of the common electronic record systems used by health care providers. Another portable device is the credit card–like "smart" card that can be encoded with a person's medical record and carried in a wallet. These are somewhat less convenient because they require a card reader to be used.

Other commercial products have been designed to provide individuals with greater personal ownership of their health information and therefore improved access to its content. Several products allow users to have an online account where their health information can be stored, which can be accessed from their desktop computer.[3] Others, such as SynChart,[4] are desktop and Web-based hybrid systems, in which the health consumer can use desktop software to maintain his or her health record, and then upload the record to a secure Web server.

The overarching purpose of these devices is to increase individuals' ability to access (and even possess) their own electronic medical records. This achievement is interrelated with the overarching goal of developing and implementing the UHR system. In essence, this system would contain the IT infrastructure—including hardware, software, standards, practices, and procedures—to allow the seamless sharing of and access to a standardized medical record format that would be universally accepted and used across the health care industry. (Ideally, this system would be adopted internationally, but this discussion is limited to developmental efforts underway for the United States.)

In his State of the Union address on January 20, 2004, President George W. Bush set the goal of achieving a federal system of computerized medical records within 10 years. In response, the Office of the National Coordinator of Health Information Technology was created, with Dr. David Brailer as its leader.[5] This health information system would cover federal-level health care organizations, such as Medicare, Medicaid, and the Veteran's Administration health system. Although there

remains a substantial amount of development work to do on this ambitious project, a city-size pilot version is currently underway. In spring 2006, Wichita, Kansas, launched the Community Health Record project, which centralizes the electronic health records (EHRs) for Medicaid recipients. The project is a joint effort among the federal government, an HMO, and a commercial IT firm, intended to improve the quality of patient care and to reduce costs and medical errors by improving health care providers' access to patient records. At this pilot stage, the medical record is an abstract of the complete record, providing a summation of key information such as patient demographic data, recent visits, medication lists, immunization records, and allergies ("Wichita Is Launch," 2006).

In time, it is hoped that the development of the federal system will facilitate the transfer of the successful technology to the health industry's private sector (American Health Information Management Association [AHIMA], 2006b). This is one of four similar consortiums developing prototype systems for what will ultimately be called the National Health Information Network ("Wichita Is Launch," 2006). The Wichita project is a necessary beginning step in the kind of collaborative process that is typical of the development of IT-based infrastructure and systems, echoing the successful development of other computerized solutions to society's needs, such as the electronic banking system or networked electronic access to library collections.

Another class of major contributors to the UHR developmental effort are the many nonprofit or professional organizations working to establish the uniform standards, vocabularies, practices, and procedures that will compose the framework to support the UHR system.[6] One of the most prominent of these organizations is AHIMA.[7] Since its founding in 1928, AHIMA has been dedicated to the improvement of health records, recognizing the link between good information access and quality of patient care. AHIMA work groups have developed highly regarded electronic health information management guidelines for best practices, and the organization also offers a free online personal health record service for consumers (AHIMA, 2006a). This organization's white papers describe and promote the issues, and the state-of-the-art solutions, pertaining to health information management.

It is important to remember that, in terms of actually building a national-level health IT infrastructure, these organizations serve in an advisory, not a regulatory, capacity. AHIMA, for example, can devise a standardized vocabulary for preferred index terms, but it has no power to mandate its adoption. The organization can only recommend and promote its use. Some commercial entities have created functioning smaller-scale, private versions of health information systems, but the U.S. Department of Health and Human Services (HSS), and its consortia, has the ultimate charge to perform the task of building the nationwide system. The result of this has been a tendency toward excessive fragmentation through localized commercial efforts to construct systems or deal with developmental issues (Aspden & Board on Health Care Services, Institute of Medicine, 2004). Nevertheless, HSS has demonstrated the greater value of a collaborative approach by opting to work with commercial and other entities in accomplishing its task.

In summary, the vision of a wide-scale, networked medical records infrastructure arises from HHS's description of "a health care industry that is consumer-centric and information rich, in which medical information follows the consumer" [rather than being tied to the provider's location] "and information tools guide medical decisions." Such a system will be designed to meet the goals of "informing clinical practice," connecting physicians, "personalizing care," and "improving the population health" (HHS, 2004). However, it is interesting to note that "preserving privacy" did not merit high enough billing to be considered a fifth goal.

The Problem of Privacy

Unfortunately, in bringing this system to fruition, patient care quality is not the only issue to be concerned with. This level of medical information access, and its accompanying enhancements to the quality of patient care, cannot be legitimately implemented in society at large without due consideration of the problem of privacy. The abuse and misuse of an individual's medical information for commercial, legal, employment, or even criminal purposes is a substantial concern in health care. Violations of patient record privacy can result in injustices such as discriminatory employment practices, invasive and embarrassing product advertising (Jacobson, 2002), and social ostracism (e.g., if a person's positive HIV status is revealed). Another threat is the potential for criminal exploitation of unprotected medical records. For example, a person suffering from a terminal illness could be targeted by a con man seeking access to his or her estate, or a married person who contracted a sexually transmitted disease could be vulnerable to blackmail. In addition, medical records contain the key ingredients of identity theft: the patient's social security number, birth date, and even credit card information. As a result of all of these concerns, the

protection of patient privacy has become the object of important legal and legislative efforts, made all the more urgent by the increasingly prevalent use of electronic IT systems for medical record keeping.

Case Law Perspectives on Information Privacy

There have been several foundational court cases in the area of health-related privacy. The review of those cases here is cursory because most of them are arguably distinct from the specific issues at play when the health information exists in an electronic format. However, because these cases compose the fundamental attitudes of the legal system toward the access and privacy conflicts being examined here, they certainly bear mentioning.

Two cases—*Roe v. Wade* (1973) and *Griswold v. Connecticut* (1965)—stand as examples of court decisions to override existing state laws that attempted to restrict reproductive freedom, using the rationale that there is an implied right to privacy of these kinds of health-related decisions that can be reasonably derived from aspects of various amendments to the Constitution. *Roe v. Wade* is the famous and still controversial case establishing the right to privacy as a basis for a woman's right to have an abortion. Although less renown than *Roe v. Wade*, *Griswold v. Connecticut* has more to contribute to this discussion. In *Griswold*, the court ruled that a state law banning the use by married couples of certain birth control methods violated a constitutionally implied "right to privacy." *Griswold* included Justice White's conception of striking a balance between protecting personal privacy and acknowledging wider interests that could justify limits on privacy.

Another case that provides historical context for the interpretation of emerging health information law is *U.S. vs. Westinghouse Electrical Corp.* (1980). Westinghouse refused to reveal the contents of its employee health records, ostensibly to protect the records' privacy, but actually it was to conceal evidence of employee illnesses resulting from the company's contaminated workplace. The court ruled that the records must be made public because public health and safety concerns outweighed concerns about the individual employees' privacy. Here, the court specifically invoked the concept of balancing the needs of society against shielding private health information and chose in favor of the former. It was determined that there was an overriding public health and safety need to make the individual health information publicly available, especially in light of the fact that Westinghouse was using the concept of medical record confidentiality as a shield to cover up its own safety problems.

Whalen v. Roe (1977) speaks directly to this discussion because it involved electronically stored medical information. In this case, the court ruled that the existence of a New York pharmacist's electronic database of patient medication records did not violate patient privacy per se but recognized the need for privacy protection of electronic health information. In adjudicating this case, the court provided an early voice on a number of the issues still being debated in the discourse on the topic today. The court recognized that databases of sensitive medical information could *potentially* lend themselves to privacy breaches but also acknowledged that such collections of data could be kept secure and therefore were not a violation of patients' privacy by their mere existence. The court also suggested the need for law or policy to be put in place to guard against improper disclosures of this information. However, Peter D. Jacobsen (2002) noted that courts have generally been lukewarm toward protecting against or punishing medical information privacy violations, in favor of supporting the use of the medical information within the contexts of cost-controlling measures for the health care industry or furthering other commercial interests.

HIPAA

As noted above, the most significant federal regulation in this area is HIPAA. It was originally targeted at allowing job-changing employees to remain covered by their health insurance (this portion is now called Title I). Later refinements (referred to as Title II) dealt with health care fraud, liability reform, and the ironically named "administrative simplification." It is this administrative simplification section that addresses the issues explored in this article (and other issues). In particular, it established national standards, forms, and protocols for the transfer of electronic health data, privacy protection for what was defined as "protected health information" (PHI), and security standards and procedures for protecting the privacy of electronic PHI. PHI is information identifiable as belonging to an individual and transmitted through electronic or other media in particular formats (Sullivan, 2004). For this discussion, any references to HIPAA below are about these sections.

This legislation created specific, and therefore complex, reporting requirements and protective procedures for what are referred to as "covered entities." These are defined as health care providers, health insurance plans, and health care clearinghouses (peripheral services having contact with the medical record, such as insurance billing subcontractors) (Sullivan, 2004). These three classes of people or organizations are the only ones

bound by the regulation, despite some confusion, such as when some law enforcement personnel have mistakenly behaved as though they were covered by HIPAA regulations and withheld information about the health status of accident or crime victims from inquiring journalists.

One additional point to note about HIPAA concerns its relationship with the many state-level statutes that also exist concerning patient information privacy. HIPAA creates a uniform federal national standard, but it does not automatically override existing state versions. In general, HIPAA creates a "floor" level of privacy regulation, but state laws that are more stringent in their protection of privacy than HIPAA are allowed to take precedence over the federal statute. There are some specific exceptions when HIPAA will prevail over a stronger state law, such as for the release of certain categories of information that is of interest to public health entities (Rieger, 2004).

At this writing, there have been few direct challenges to the constitutionality of HIPAA's privacy standards. Two of these cases argued that HIPAA's privacy standards violated specific Amendments. *Association of American Physicians and Surgeons v. U.S. Dept. of Health and Human Services* (2002) alleged that the privacy standard violated the Fourth Amendment by allowing government entities unlimited access to individuals' medical records but was dismissed because the court felt HIPAA had been too recently implemented for this constitutional issue to be decided (Bilimoria, 2002). In another, *Citizens of Health v. Thompson* (2004), the court ruled that HIPAA privacy regulations do not violate the First, Fourth, Fifth, or Ninth Amendments (Ignatova, 2006). In a third, *South Carolina Medical Association v. Thompson* (2003), an attempt to declare HIPAA unconstitutional based on both its congressional-mandate origin and its criminal penalty portions likewise failed (Ignatova, 2006).

Other court activity specifically regarding HIPAA pertains to interpreting the significance of its ambiguous areas or pitting it against existing state laws about health information privacy. One recent (March 2006) example of this was an Ohio Supreme Court ruling that HIPAA's shield against the disclosure of PHI did not extend to the Cincinnati Public Health Department's records on the presence of dangerous lead in a number of homes that they had inspected. The court allowed the release of these records to a newspaper because precedence was given to the state's Open Records Law. Also, it was judged that the information failed to meet the test of PHI because the records did not specifically identify minor residents of the homes and the information was not the product of medical treatment (Reporters Committee for Freedom of the Press, 2006).

Although freedom and privacy of information are not new issues, the electronic health information environment, and its regulation by HIPAA, composes a relatively new frontier, so the themes and directions of legal actions in this area are still in a formative stage. June M. Sullivan (2004) anticipated that HIPAA will ultimately spawn substantial litigation, both in small-stakes actions brought by individuals for particular breaches of privacy and in high-stakes class-action filings for the kinds of massive privacy breaches that can be easily conceived of in the electronic information setting. She noted that HIPAA creates a myriad of duties and contractual obligations between the various covered entities and health consumers, which means plenty of opportunities for those duties and contracts to be breached. She also points out that HIPAA's federal-level orientation does not preclude state law–guaranteed private rights of action. She noted that various legal scholars have ventured that the volume of HIPAA-related litigation might ultimately rival "tobacco litigation, breast implant litigation, and asbestos litigation."

HIPAA is a very complex piece of legislation, with an important and multifaceted purpose. A more thorough explication of it is beyond the scope of this article but is readily available to readers in two particularly useful books. Sullivan's (2004) handbook offers a systematic deconstruction of all of the privacy portions of HIPAA, with the overarching purpose of aiding the accuracy of compliance by covered entities. Michael Doscher's (2003) book explains and describes HIPAA using an accessible outline-driven style. This work, written from a managerial or operational point of view, also offers detailed, pragmatic suggestions for policies and procedures to achieve HIPAA compliance on an organizational level.

Perspectives on Criticisms of HIPAA

The most pervasive criticism of HIPAA seems to be based on a philosophical disdain for statutory regulation or bureaucratic solutions in general. HIPAA is frequently criticized for excessive complexity, for spawning additional bureaucracies, for excessive ambiguity (e.g., with interpreting the "minimum necessary" rule; Kapushion, 2004), for imposing undue financial and administrative burdens on covered entities, and for making health care more expensive and less responsive to consumer needs (Jacobson, 2002).

Some critiques of HIPAA approach from an economic perspective. For example, Meredith Kapushion (2004) argued that HIPAA's regulatory approach to protecting information privacy suffers from its generic quality and prevents the focus on consumer preferences and individual decision making that a free market approach would allow. This argument is based on the idea that individual health consumers have different preferences in the degree of information privacy they desire and different valuations of what they feel health information privacy is "worth." Kapushion lamented that HIPAA's uniform regulation forces all health consumers to place a high value on privacy protection and feels that even an imperfect market would function better than this regulatory solution.

In contrast, other legal writers express skepticism that the market alone is up to the challenge of protecting medical information privacy (e.g., Solove, 2004). This opposing argument asserts that market-based controls (or the closely related contractual law–based approaches to privacy) are powerless to prevent the abuse of individuals' private records by third parties. Another reason is that when commercial entities use their own privacy policies (which are actually contractual approaches), consumers are often left with no bargaining leverage to negotiate or enforce compliance with the policy.

Daniel J. Solove (2004) further argues that, unlike with conventional goods and services, market forces alone cannot effectively curtail violations of the privacy of individuals' electronic information because the online environment allows these offending bureaucracies' and commercial entities' violations to occur, often without the victims being aware that they have happened. It is impossible for consumers to bring economic pressure to bear on the situation when they do not realize they have been wronged, much less by whom.

Interestingly, although Solove (2004) attacks the economic-oriented criticism of HIPAA, he is also dissatisfied with HIPAA because of his discomfort with large-scale legislative regulation. Instead, he asserts that electronic information privacy should be protected through a system of consumer-specified permissions to release information, enforced through judicial review and legal action. Although this proposal is logical, it is unclear how our already overloaded courts would cope with this additional workload. This alternative to HIPAA may just substitute a legal bureaucracy for a governmental one.

Taken on balance, it seems that more of these sources came to bury HIPAA than to praise it. Few would deny that HIPAA is unwieldy, is complicated, is extremely costly, and has probably caused a lot of administrative people in the health care industry to put in too many overtime hours. However, HIPAA has succeeded in one way—it has started a very big, important, and probably unstoppable ball rolling, a ball that might not have been put into motion any other way. There was a vital need for society to address, in practical terms, the issues of access and privacy that have emerged out of the technological and informational revolutions in the practice of medicine. HIPAA, with its ubiquity of approach, legal power, imposition of deadlines, and breadth of reach, has served as an undeniable force in addressing the tough issues involved in standardization of information and electronic privacy in medical records. It seems unlikely that the alternative approaches (market forces, judicial reviews, or even just doing nothing on a grand scale) would have made so much progress happen so fast. HIPAA is no doubt full of flaws, but it has created action, for better or for worse.

Technological Approaches to Safeguarding Privacy

The nostalgic tone of those who hearken back to the days of a single paper-only medical record, housed solely in the files of the family doctor, seems to suggest that paper medical records are "safe" whereas electronic ones are not. This belief is a fallacy. Although EHRs may be more vulnerable to larger-scale privacy breaches, they make it easier to find out about improper disclosures. EHR systems can be designed to include disclosure tracking logs that can provide an electronic record of to whom any disclosures of PHI were made. Audits of these logs can be used to follow up on unauthorized disclosures (AHIMA, Health Information in a Hybrid Environment Work Group, 2006). In contrast, discreetly made improper disclosures from paper records can conceivably occur without anyone ever finding out about them.

An in-depth discussion of technology-based solutions for safeguarding information privacy could easily fill multiple articles and is beyond the scope of this one. However, some of the most promising ones warrant a mention, if only to provide a factual perspective on the need for including a substantial technological component in any solutions to the problem of health information privacy.

Doscher (2003) said that any technological solution needs to interface with the physical plant and personnel-based aspects of the organization involved. He also pointed out that most covered entities are currently

unable to comply with HIPAA's technical security guidelines. Among the technological compliance goals he suggests are

- Encryption (to the highest supported level) of data being transferred within an organization or to other covered entities, and not just for those data using Internet transfer protocols.
- Storage of all HIPAA-related documents in a secured data warehouse (electronic archive).
- Active archiving of all access and disclosure logs, so records are kept of who received disclosed data.
- The use of biometrics (e.g., fingerprint ID recognition) to secure access to computers and networks, chart and information storage devices, and even the employee parking lot and entrance.
- Software should use pop-up warning screens that are keyed to patient-specified privacy protocols so that inadvertent disclosures are more easily avoided.

Contrasting Perspectives

A comparison of writings about HIPAA reveals the contrast in perspectives on health information privacy that can be found in the legal literature versus the health or health information management literature. Many of the legal writers who addressed HIPAA were strongly oriented to the protection of privacy while discounting or ignoring potential care-related problems with restricting access to health information. For example, Fred Cate (2002) expressly commented on the obscurity of the "alternative" position in the debate on privacy, asserting that any benefits from increased information flows are indistinguishable from our everyday lives. Kapushion (2004) saw an ominous threat to privacy in HIPAA's rule that medical record transactions use a standardized format to facilitate uniform data collection. Although she recognized that this standardization promotes cost-efficiency, there is no expressed awareness of its value in supporting quality patient care. In addition, some of the legal writers who did specifically acknowledge the aspects of patient welfare or quality of care sharply discounted the importance of this value in comparison to preserving privacy (e.g., Jacobson, 2002).

In contrast, writers from the health care or health information management disciplines emphasize the importance of using IT, ultimately in the form of the national health information infrastructure (or some analogous concept of a UHR system) to solve existing problems of patient safety and to improve the quality of care delivery (e.g., Aspden & Board on Health Care Services, Institute of Medicine, 2004). Authors in this genre do recognize that the diffusion of EMRs creates significant privacy concerns (Dennis, 2000); however, privacy protection tends to be treated as one item in a laundry list of many important, but potentially solvable, difficulties to correct in the course of building the system, along with standardization of preferred vocabulary terms and agreement about file transfer protocols. Here, privacy is not as much of a focal point as in the legal literature.

It is possible that this apparent divergence in perspectives, or at least priorities, could have implications for all efforts to address either or both problems. If one accepts that large-scale problems are better solved through overt collaboration than through independent, potentially oppositional efforts, it is arguable that the first step in coordinating disparate efforts is mutual recognition that the other perspectives exist. This viewpoint inspires the model described below.

The Equilibrium Metaphor

Balancing imagery describes one of the most fundamental purposes of law, to seek a fair compromise between oppositional positions or values. For example, the criminal justice system seeks the optimum balance of individual freedom of action, with social control and order. This concept of equilibrium as a goal of the law is symbolically represented most pervasively by the "scales of justice" image. Language recognizing the need for a "balancing" solution frequented the decisions in the foundational medical privacy court cases, such as *United States v. Westinghouse* and *Roe v. Wade*. Similarly, the concept of equilibrium as a goal pervades the discourse on privacy of EHRs, in which most policy makers and scholars recognize the existence of a trade-off of values between access to information and the protection of an individual's privacy.

However, the binary simplicity of a scale metaphor actually understates the complexity of the value conflicts that underlie this problem. Instead, a more inclusive and interactive model is needed to conceptualize the various tensions that this interplay of desirable values creates (see appendix). The need for an equilibrium relationship between the oppositional positive values is better represented by two orthogonal continua that define four quadrants of beneficial outcomes. The information flow–privacy protection continuum represents the tension between the positive value of increasing the free flow of electronic health information versus the equally important objective of safeguarding privacy. If steps are taken to free up the flow of electronic health information, by removing barriers to accessing that

information, the information will become known by a larger number of people, therefore reducing the privacy of that information. In turn, if the medical information resides in a system that contains many barriers to access, few people will be able to obtain that information, and the privacy of that information will be more secure. Simply put, increasing information flow will result in a loss of privacy for that information, whereas increasing the privacy controls on that information will reduce its availability. The second dimension of the model, the needs continuum, illustrates the phenomenon that there can often be an oppositional relationship between the needs of individuals and the needs of the collective society.

Each of the quadrants formed by the intersection of these two continua represents a set of sought-after outcomes that are improvements in the human condition, as it relates to health care information. The quadrant formed by the conjunction of the individual needs–information flow continua represents the health care priorities area of the model. Here, the values of maximizing ease of information flow and the priorities of individuals (both health consumers and health care professionals) are emphasized. This is the situation reflected in the emergency room scenario described above. Under these conditions, optimization of health information access and a prioritizing of patient welfare lead to these outcomes: a high degree of informed medical decision making and the minimization of medical errors and subsequent harm to patients.

The public health effectiveness quarter of the model entails the conditions where information flow and societal needs converge. Societal needs in this context reflect the collective aspects of a freer health information flow. Positive outcomes in these circumstances include the access to aggregated health data that are needed to support medical and academic research and successful efforts by public health personnel to control and prevent disease.

A third quadrant in the model pertains to individual security, where the values of individual needs and privacy protection converge. In this context, the preservation of individual privacy is paramount, a value priority that is emphasized in much of the legal literature on medical information privacy. The positive outcomes from this sector are the much-discussed personal safety and security and the sanctity of individual freedom. In addition, there is an improvement in the quality of disclosure by patients to their health care providers. Individuals feel more comfortable about revealing sensitive or embarrassing information to their providers when they believe that the information in their medical records will remain confidential (Doscher, 2003).

The confluence of societal needs and privacy protection yields the final portion of the model: the e-health development quadrant. When these values are emphasized, both online and brick-and-mortar health businesses flourish and compete for an expanding customer base, as health consumers and health care providers venture into using IT-based health innovations, such as health information security consultants or telemedicine applications. The success of these kinds of e-health businesses is contingent on the presence of an aggregate-level confidence that the e-health industry has achieved a sufficient level of privacy security to justify the risks perceived to accompany the adoption of these innovations (Doscher, 2003).

The purpose of this model is to illustrate the importance of considering the "big picture," as stakeholders coming from various perspectives attempt to address the issue of electronic health information and privacy. The continued evolution of electronic health information systems is a given because of the complexity of modern health care delivery and economic management. The real questions lie in what the nature of the solution will be, which perspectives will be given priority, and which risks will be neglected. Health information–oriented policies and procedures that arise only from the perspective of valuing individual privacy will result in deleterious effects on the quality of health care and even direct harm to patients from "acute" information shortages. Likewise, if only the perspective of individual information access is valued, individuals will suffer from emotional trauma and discrimination as their privacy is invaded. If voices advocating society's need to access aggregate health data are silenced, the advance of medicine through research will be slowed and the efficacy of public health to safeguard the public may be dangerously curtailed.

Even the legitimacy of the commercial side of health care needs to be acknowledged because health care is ultimately an industry, albeit one with a humanitarian purpose. Sustaining quality and innovation in health care requires massive economic input, and e-health represents the advancing edge of that industry.

In summation, it is argued here that a proper equilibrium in the solution can only be reached (or even approached) if policy makers, legislators, and all the other stakeholders both are aware of and have a respect for perspectives other than their own.

Discussion and Recommendations

Based on this review of the competing and conflicting objectives of enhancing health care information flow while protecting individual information privacy, here are

some specific recommendations to consider in the ongoing attempt to achieve the proper blending of these worthwhile goals:

Record ownership: Reframe the ownership of EHRs through policy and legislation, so that an individual is seen as the owner of his or her universal electronic medical record, with health care providers as primary custodians of the record and the remaining kinds of HIPAA-covered entitles as privileged users of the record. This change is appropriate because EHRs are not tied to a particular institution (like paper records were); instead, they are keyed on an individual.

Focus on the individual: The efforts of policy makers, legislators, administrators, and commercial interests should focus on advancing the concept of the health consumer as an active stakeholder in the management of electronic health information. Technology and health management information systems can be designed to emphasize an individual's ownership of his or her own medical information by facilitating his or her access to the record and by enabling the individual to contest, revise, or "quarantine" portions of the record from use by specified classes of users.

Aggregation of record users: The EHR should allow its individual owner to exclude the access and use of the information by *classes* of users. For example, the individual could prohibit the record's use by any commercial entities or even by those touting specific classes of medication. This approach would enable individuals to "opt in" to being contacted by the types of commercial entities from which they are interested in hearing while avoiding any and all of the others. Health consumers should be able to "untarget" themselves from uninvited efforts of health product advertisers.

Advertising regulation: These changes in information system design would require supporting changes in advertising regulation to enforce compliance by health product marketers. Regulators should recognize and communicate to the advertising industry that health products, particularly medicines, compose a unique commodity group that is inappropriate for a targeted, direct-to-consumer approach because their use and purchase decisions demand mediation through a licensed medical professional. Increasing regulation of the targeted, direct to consumer advertising for health products would substantially reduce the incentive for commercial entities to obtain and use information from individual EHRs and therefore help to preserve patients' privacy.

Physicians as gatekeepers: Health care industry marketing efforts do not have to be unduly restrained by this regulation. Commercial entities could still legitimately publicize their products to physicians and health care providers directly, allowing those medical professionals to function as gatekeepers in deciding whether or not to pass the information (via brochures or samples) on to the appropriate patients. This recommendation is not meant to be a step "backward" from the more recent movement to empower health consumers; it simply provides another layer of "protection" for the patient from unwanted commercial use of his or her health information. Direct consumer awareness of health products or medicines could still be legitimately achieved through the continued use of general print or broadcast advertising or even untargeted online ads.

Record design: The design of the UHR will no doubt evolve and improve over time. On a technical level, the record should be designed in such as way as to facilitate the splitting off of medical content data from the individual identification data so that the content that academic and medical researchers, marketers, and public health statisticians have a legitimate interest in can be obtained for aggregated use while minimizing accidental revelations of personally identifiable content.

Professional guidance: The health care industry and professions must recognize the need to define a new class of medical professional—health information management counselors. This need arises from the computerization of medicine and health information, which has added an entire new technological context to the delivery of health care, one with which current classes of health professionals have neither the time nor the expertise to contend.

These health information counselors would function in the style of social workers or genetic counselors (e.g., Wang, Gonzalez, & Merajver, 2004) but with a focus on facilitating the interaction of the patient and his or her electronic medical record. They would act as patient advocates and consultants to advise health consumers on how to effectively manage their UHR. For example, the counselor could consider a particular patient's circumstances and advise him or her on the appropriate choices to make regarding opting in on product advertising or whether he or she should challenge or quarantine a portion of his or her record. The counselor could also function as a failsafe step to help insure that the history and symptomatic information entered in the UHR by medical

professionals accurately reflects what the patient intended to communicate. These counselors would be especially important for disadvantaged patients without either the technology access or IT skills to effectively manage their own UHR. To be effective, the counselors' training should probably involve an interdisciplinary melding of health and medicine, information science, and law.

Conclusion

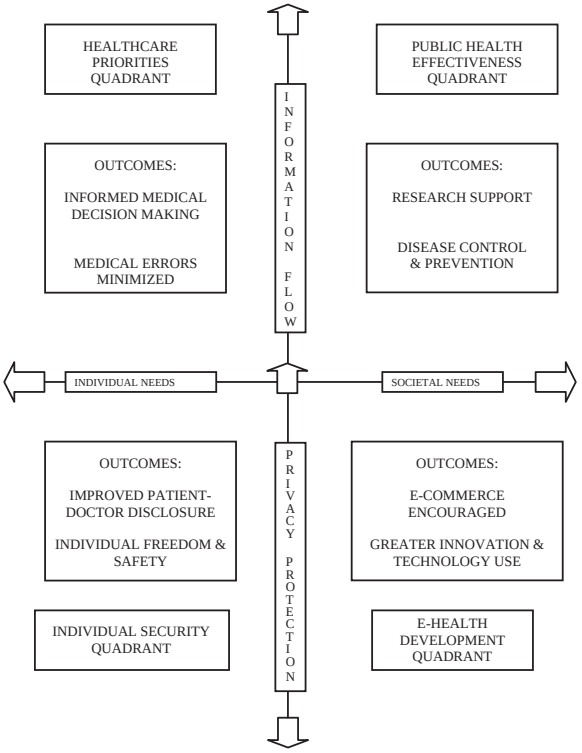
The ultimate solution to the problem of reconciling the values of health information access and privacy will necessarily be technology driven. The practice of medicine, and the delivery of health care, will continue to be increasingly data laden, so that instantaneous, point-of-service access to a patient's health record will be even more inextricably bound up with the health care provider's duty to properly care for the patient. The solution is probably less a fixed goal than a process—continual improvement toward the gold standard of an accurate, seamlessly accessible, and appropriately privacy-protected UHR. However, it is vital to remember that good technological solutions are achieved only when they arise out of appropriate human interactions. In this case, that interaction needs to reflect the interests and contributions of people coming from each of the four perspectives identified above.

Over time, many scholars have used transportation metaphors to address issues involving human communication and information exchange (Carey, 1989). Perhaps this is also appropriate when considering the problem of developing a safe and effective system to support UHRs. No reasonable person would argue that the complex amalgamation of roads, highways, and laws that compose our modern traffic system should be abolished because it has failed to eliminate traffic accidents or prevent fatal car crashes. Instead, it is widely recognized that the system is flawed but basically functions well, considering the complexity of the task involved in allowing vast populations to reach their destinations in a reasonable amount of time. The social and economic benefits of the traffic system validate its existence, despite the costs to society and to some individuals of its inevitable failures.

The same kind of society-level expectations are also appropriate for the developing system to support UHRs. The societal and individual-level benefits discussed above are sufficiently great to warrant living with the risks that efficient electronic information flow pose to the privacy of individuals' health information. All of the stakeholders involved in developing and regulating this vital branch of IT infrastructure must face the reality that their efforts will continually advance and improve a system that will inevitably be imperfect yet superior to any alternatives. As the solution moves closer to the most desirable vision of the UHR, privacy protection and information flow will ultimately become mutually supportive forces in a symbiotic cycle, supporting both individual and society-level needs rather than antithetical endpoints on a continuum.

Appendix

Model of the Electronic Information–Privacy Protection Interaction



Notes

1. One of the leading brands of identity chips for pets is AVID (http://www.avidmicrochip.com).
2. CapMed's Personal HealthKey (http://www.capmedphr.com).
3. Examples of these online information repositories are MyPersonalMD (http://www.personalmd.com) and HealthTracer (http://www.healthtracer.com).
4. Synchart (http://www.synchart.com).
5. For more about the work of the Office of the National Coordinator of Health Information Technology, see http://www.hhs.gov/healthit.
6. For example, Connecting for Health. See http://www.connectingforhealth.org for more information on their development efforts, including a video overview of their common framework.

7. American Health Information Management Association home page, along with access to their online white papers on many of their component tasks in building the architecture of a universal health record system, is found at http://www.ahima.org.

References

American Health Information Management Association. (2006a). *AHIMA and AHQA partner to advance healthcare quality improvement*. Retrieved April 10, 2006, from http://www.ahima.org/press/press_releases/06.0322.asp

American Health Information Management Association. (2006b). *The health information management role in patient safety and quality of care*. Retrieved April 10, 2006, from http://www.library.ahima.org

American Health Information Management Association, Health Information in a Hybrid Environment Work Group. (2006). *The complete medical record in a hybrid electronic health record environment, Part II: Managing access & disclosure* (AHIMA practice brief). Retrieved April 10, 2006, from http://www.ahima.org

Aspden, P., & Board on Health Care Services, Institute of Medicine. (2004). *Patient safety: Achieving a new standard for care*. Washington, DC: National Academies Press.

Association of American Physicians and Surgeons v. U.S. Dept. of Health and Human Services, H-01-2963 (June 17, 2002).

Bilimoria, N. M. (2002). Contending with HIPAA privacy standards in Illinois. *Illinois Bar Journal*, *90*, 414.

Carey, J. W. (1989). *Communication as culture: Essays on media & society*. Boston: Unwin/Hyman.

Cate, F. (2002). Principles for protecting privacy, *Cato Journal*, *22*(33), 34-36.

Citizens of Health v. Thompson, 03 E.D. Pa. 2267 (2004).

DeMoss, J. (2006, April 2). USDA program introduces nationwide database for livestock. *Ogden Standard-Examiner*. Retrieved April 10, 2006, from http://www.redorbit.com/news/science/457733/usda_program_introduces_nationwide_database_for_livestock/index.html

Dennis, J. C. (2000). *Privacy & confidentiality of health information*. San Francisco: Jossey-Bass.

Doscher, M. (2003). *HIPAA: A short- and long-term perspective for health care*. Chicago: AMA Press.

Griswold v. Connecticut, 381 U.S. 479 (1965).

Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d (1996).

Ignatova, K. (2006, February). *HIPAA's privacy rule: Adding oil to the long-burning fire between personal privacy and public interest*. Paper presented at the 28th Annual Research Symposium, University of Tennessee, College of Communication & information, Knoxville.

Institute of Medicine. (1999). *To err is human: Building a safer health system*. Washington, DC: Author.

Jacobson, P. D. (2002). Symposium: Modern studies in privacy law: National health information privacy regulations under HIPAA. *Minnesota Law Review*, *86*, 1497.

Kapushion, M. (2004). Hungry, hungry HIPAA: When privacy regulations go too far. *Fordham Urban Law Journal*, *31*, 1483.

Reporters Committee for Freedom of the Press. (2006, March 24). *Open records law trumps HIPAA in records request case*. Retrieved April 4, 2006, from http://rcfp.org/news/2006/0324-foi-openre.html

Rieger, K. S. (2004). Federal health information privacy requirements. In S. S. Sanbar, M. H. Firestone, & F. Buckner (Eds.), *Legal medicine* (6th ed., pp. 214-218). Philadelphia: C. V. Mosby/Elsevier.

Roach, W. H., Jr., & Aspen Health Law and Compliance Center. (1998). *Medical records and the law* (3rd ed.) Gaithersburg, MD: Aspen.

Roe v. Wade, 70 U.S. 18 (1973).

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. New York: New York University Press.

South Carolina Medical Association v. Thompson, 327 F. 3d 346 (4th Cir. 2003).

Sullivan, J. M. (2004). *HIPAA: A practical guide to the privacy and security of health data*. Chicago: American Bar Association.

U.S. v. Westinghouse Electrical Corp., 80 U.S. App. 1269 (1980).

U.S. Department of Health and Human Services. (2004, July 21). *The decade of health information technology: Delivering consumer-centric and information-rich health care: Framework for strategic action*. Retrieved April 4, 2006, from http://www.hhs.gov

Wang, C., Gonzalez, R., & Merajver, S. D.(2004). Assessment of genetic testing and related counseling services: Current research and future directions. *Social Science & Medicine*, *58*, 1427-1444.

Whalen v. Roe, 75 U.S. 839 (1977).

Wichita is launch city for electronic medical records initiative. (2006, April 7). *Wichita Business Journal*. Retrieved April 8, 2006, from http://www.bizjournals.com/wichita/stories/2006/04/03/daily34.html

Kitty McClanahan is a doctoral student in the School of Information Sciences, College of Communication and Information, at the University of Tennessee. She is studying health information and public health-related information behavior.

Requirements Eng (2010) 15:119–137
DOI 10.1007/s00766-009-0089-5

SPECIAL ISSUE—SECURITY REQUIREMENTS ENGINEERING

Evaluating existing security and privacy requirements for legal compliance

Aaron K. Massey · Paul N. Otto · Lauren J. Hayward · Annie I. Antón

Received: 7 November 2008 / Accepted: 21 October 2009 / Published online: 13 November 2009

Abstract Governments enact laws and regulations to safeguard the security and privacy of their citizens. In response, requirements engineers must specify compliant system requirements to satisfy applicable legal security and privacy obligations. Specifying legally compliant requirements is challenging because legal texts are complex and ambiguous by nature. In this paper, we discuss our evaluation of the requirements for iTrust, an open-source Electronic Health Records system, for compliance with legal requirements governing security and privacy in the healthcare domain. We begin with an overview of the method we developed, using existing requirements engineering techniques, and then summarize our experiences in applying our method to the iTrust system. We illustrate some of the challenges that practitioners face when specifying requirements for a system that must comply with law and close with a discussion of needed future research focusing on security and privacy requirements.

Keywords Security requirements · Privacy requirements · Legal compliance · Refactoring requirements

A. K. Massey (✉) · P. N. Otto · L. J. Hayward · A. I. Antón
Department of Computer Science,
North Carolina State University, Raleigh, NC, USA
e-mail: akmassey@ncsu.edu

P. N. Otto
e-mail: pnotto@ncsu.edu; paul.otto@law.duke.edu

L. J. Hayward
e-mail: ljhaywar@ncsu.edu

A. I. Antón
e-mail: aianton@ncsu.edu

P. N. Otto
School of Law, Duke University, Durham, NC, USA

1 Introduction

> All that may come to my knowledge in the exercise of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal.
> The Hippocratic Oath

Although centuries old, the well-known Hippocratic Oath[1] still influences our cultural understanding of ethics in healthcare. The Hippocratic Oath may be known best for its "do no harm" clause, but the privacy promise quoted above is extremely motivating to information security and privacy professionals, particularly in the field of medicine. Perhaps partly to fulfill the ancient privacy promise in the modern age, the United States passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[2] The resulting HIPAA regulations govern patient health information usage by providing detailed security and privacy procedures to support the practical needs of insurance companies, healthcare providers, law enforcement and other organizations that have a bona fide need for access to patient health information.

Although HIPAA's focus is broader than computer-based systems, it was intentionally constructed to cover them. Healthcare facilities have been using computers to manage basic health information, such as patient admission

[1] http://www.nlm.nih.gov/hmd/greek/greek_oath.html.

[2] Pub. L. No. 104–191, 110 Stat. 1936.