Journal of Biomedical Informatics 43 (2010) S51–S55

Contents lists available at ScienceDirect

Journal of Biomedical Informatics

journal homepage: www.elsevier.com/locate/yjbin

Ethical, legal and social issues for personal health records and applications

Reid Cushman [a,*], A. Michael Froomkin [b], Anita Cava [c], Patricia Abril [c], Kenneth W. Goodman [d]

[a] University of Miami Health System, School of Medicine, Department of Medical Information Technology, 1051 N.W. 14th Street, Miami, FL 33136, United States
[b] University of Miami School of Law, P.O. Box 248087, Coral Gables, FL 33124, United States
[c] University of Miami School of Business Administration, Jenkins Building 323-F, P.O. Box 248022, Coral Gables, FL 33124, United States
[d] University of Miami Ethics Programs, Dominion Tower, 1400 N.W. 10th Ave., Suite 916 (M-825), Miami, FL 33136, United States

ARTICLE INFO

Keywords:
Ethics
Personal
Health
Record
Application
PHR
PHA
ELSI

ABSTRACT

Robert Wood Johnson Foundation's Project HealthDesign included funding of an ethical, legal and social issues (ELSI) team, to serve in an advisory capacity to the nine design projects. In that capacity, the authors had the opportunity to analyze the personal health record (PHR) and personal health application (PHA) implementations for recurring themes. PHRs and PHAs invert the long-standing paradigm of health care institutions as the authoritative data-holders and data-processors in the system. With PHRs and PHAs, the individual is the center of his or her own health data universe, a position that brings new benefits but also entails new responsibilities for patients and other parties in the health information infrastructure. Implications for law, policy and practice follow from this shift. This article summarizes the issues raised by the first phase of Project HealthDesign projects, categorizing them into four topics: privacy and confidentiality, data security, decision support, and HIPAA and related legal-regulatory requirements. Discussion and resolution of these issues will be critical to successful PHR/PHA implementations in the years to come.

1. Introduction

Personal health records (PHR) have been lauded for their potential to improve the efficiency of healthcare and support the individual patient – "empowering" devices that "everyone should have" [1,2]. A rapidly expanding set of organizations is offering consumers personalized recordkeeping and support services for health-related matters, Google and Microsoft among them. The growing popularity of PHRs necessitates a critical evaluation of the ethical, legal, and social issues (ELSI) they present. This article summarizes the ELSI commonalities observed in Project HealthDesign projects [3].

2. Common ELSI issues

There are myriad ways to partition the ELSI landscape for PHR [4–6]. We group the discussion here into four areas: privacy and confidentiality, data security, decision support, and the legal-regulatory regime for health data (see Table 1).

3. Privacy and confidentiality

As in the world of institutional electronic medical records (EMR), inappropriate third-party access to PHR data is a threat to individuals' privacy. Unauthorized access and disclosure of health information can result in insurance and employment discrimination, as well as embarrassment and other dignitary harms. PHRs engaging in data sharing with institution-based records are particularly susceptible to leaks. While recipient institutions may include traditional insurers and healthcare providers duty-bound by privacy law, the emergence of new often-unregulated commercial actors such as websites and commercial entities elevates privacy concerns.

3.1. Granular control over disclosure

One of the most appealing features of PHRs is the ability for consumers to easily share their health data with family and other caregivers. However, many PHRs provide limited ability to filter or control the particular PHR data elements to be shared, even with primary caregivers and family members. Given potential access by several layers of entities with access to the information, this lack of granularity-of-control poses an additional privacy concern.

Patient withholding of data from professional healthcare providers raises obvious care and liability issues. If a healthcare practitioner by law or custom comes to rely on PHR data as authoritative, any substantive omission or misstatement jeopardizes the quality of care practitioners can provide. While these issues already occur in the prosaic context of today's standard intake

* Corresponding author. Fax: +1 305 243 6417.
E-mail address: rcushman@med.miami.edu (R. Cushman).

1532-0464/$ - see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.jbi.2010.05.003

Table 1
Summarizing the ELSI categories and their applicability to PHRs/PHAs.

Privacy and confidentiality	• Granular control over PHR disclosure • Ubiquitous monitoring to generate PHR data • Cohort effects and vulnerable populations using PHRs • Social networking reliance of PHRs • Legal uncertainty regarding non-traditional actors
Data security	• Challenges of PHR data protection in distributed environments
Decision support	• By PHAs using PHR data, provided to patients sometimes without clinical intermediaries and in extra-clinical settings
Legal-regulatory environment	• Multiple federal requirements and state requirements for PHR-based data and new environments, all evolving

disclosures, the absence of physical contact between the healthcare provider and patient can exacerbate the issue.

3.2. Ubiquitous monitoring

The disclosure stakes are raised by PHRs' potential to harvest and store a wide range of data when paired with ambitious personal health applications (PHA). Ambitious implementations contemplate a regime of ubiquitous medical monitoring, from which data might be filtered to a PHR via multiple sensors installed in the patient's own house or on their body. Such comprehensive, longitudinal data acquisition potentially enhances the quality of care; however, this could be a harbinger of round-the-clock medical surveillance of the most personal and private of spaces, one's own body.

3.3. Cohort effects and vulnerable populations

Distinctive privacy issues arise in vulnerable populations, but particularly here, where extensive data capture may be immortalized after PHR data is migrated into a centralized store – be it an electronic medical record (EMR) or a social networking site. Younger patients are, to generalize broadly, more comfortable sharing personal details. Under what circumstances should minors' data transfers require parent/surrogate consent? Should a (perceived) parental failure with respect to PHR data management – be it "too much" or "too little" data sharing – expose parents to social or legal liability? The same issues obtain for elderly patients, who might have impairments that reduce their ability to make informed judgments about data collection and sharing.

3.4. Social networking

Many Project HealthDesign efforts leveraged social networking as a mechanism for information-sharing, peer counseling and general encouragement, particularly with respect to managing chronic diseases. A few were particularly dependent on extensive self-disclosure to social networking communities, including via cell phone use, phone texting capture, among others. As with conventional medical histories, a range of biosensor, weight and other data from the "ubiquitous" sensory environment could be shared in social networks. Social networking involving information-sharing of this kind raises the need for augmented cohort trust and confidentiality, as well as system architecture that supports it.

It is also important to note that personal health disclosures include data about or relating to family members. It is one thing to decide to voluntarily disclose one's own information; it is quite another to reveal someone else's stigmatizing disease or condition. This issue will grow in importance as genetic information becomes a greater part of patient records and enters the domain of PHRs.

3.5. Legal uncertainty

The Health Information Technology for Economic and Clinical Health Act (HITECH) has now extended some privacy and security protections of the Health Insurance Portability and Accountability Act (HIPAA) to PHR providers [7,8]. Even so, PHRs and PHAs raise still-unsettled legal questions regarding about the proper expectations, rights, and duties of the patient and any caregivers. Laws generally cease to protect privacy if otherwise protected information has been disclosed to another outside of a legally-recognized duty of confidentiality such as doctor–patient or attorney–client. Laws sometimes protect even voluntarily disclosed information if the parties have a special relationship of trust, or (in rare cases) if the information is otherwise secret and shameful. This leaves several confidentiality uncertainties for PHR-generated data that has been freely disclosed on, say, a social networking site. The disclosure may have had a specific contextual limitation with an expectation of privacy outside of that context. But such an expectation is not deemed reasonable in the current legal environment.

Online networking is essentially unregulated. Commercial providers/ISPs have no duty to users in the absence of a healthcare provider relationship. This means a commercial provider of a social networking site can delete information, lose information, and delete a user profile without repercussion or user recourse. The stakes for such issues are raised if social networking is a critical vehicle for health information exchange. Numerous questions remain regarding commercial PHR providers, where information is collected by many with different goals. What benefits can legitimately accrue to the PHR provider, rather than the patient, from such arrangements? What sorts of benefits are prohibited? What constitutes "undue influence" or "improper disclosure" in such contexts?

4. Data security

Data security issues arise in any project requiring storage or manipulation of sensitive personal information. PHR designs often make use of portable devices as storage and application platforms, where the data security challenges are even more formidable. Sufficiently robust authentication and access controls must be provided in health information settings, given the sensitivity of the data at issue. Balancing protection against ease-of-use is one of the greatest challenges for institutional EMRs, particularly where EMRs are robustly networked. It is even more challenging for PHRs, where some users may be physically and/or mentally impaired. As noted, access limitation is inherently complex because of the range of PHR data and the many parties who may wish (or need) to have access to it. Segmentation of data into appropriate spheres of protection raises a considerable challenge even in an institutional EMR world. Personalization of security, along with the other aspects of personalization of PHRs, makes it even more difficult. HITECH's new requirements just begin to address these issues.

5. Decision support

Many Project HealthDesign PHRs feature decision support in the form of reminder, advice and treatment recommendations. Questions concerning backup, error detection and management, faulty input and other classic issues in decision support literature on EMRs now recur with PHRs. Sites' self-management tools raise yet more issues, including appropriate use and users, the need for human oversight and intervention, and the tolerance of various types of predictive error. This occurs whether the decision support is presented as authoritative ("take this pill now") or requires data analysis by non-clinicians (patients, caregivers). It also raises is-

sues of unintended discovery and putative duty to warn of medical risk and to whom such a duty might apply. These devices are complex, so it is necessary to ask whether the average parent or guardian would have the time and ability to "supervise" the decision support when applied to a vulnerable population.

Some sites are exploring the use of embedded clinical guidelines in PHR-mediated decision-making. Practice guidelines as a cornerstone of evidence-based practice lend themselves well to decision support – while amplifying challenges related to computational decision-making and clinical assessment. Future "smart medical homes", also contemplated by some sites, will amplify these issues. Automated decision support technology begs the question of appropriate limits for patient determination of treatment in a variety of diagnostic settings.

Risk disclosure could be a significant issue from the moment patients are presented with such platforms, even with modest decision support functions like behavioral reminders – e.g., "exercise today"! Such reminders generally raise fewer risks than, say, a medication choice, but pose their own concerns. What if the person is not feeling well today – and the PHR is not sophisticated enough to detect that "condition"? It is natural to assume that such behavioral reminders would be targeted at an older, sedentary population. But calendaring and reminder systems based on activities of daily living for the young also introduce a so-far unaddressed domain of inquiry regarding appropriate system use.

6. Legal-regulatory requirements

The general inapplicability of today's laws to PHRs is a concern, especially given the ever-expanding possibilities for PHR data misuse with respect to potentially stigmatizing diseases, conditions and medications. As noted, HITECH does extend some HIPAA requirements to PHRs. Many states as well as HIPAA (modified by HITECH) have instituted "data breach" notification laws. These measures also increase security requirements on organizations that hold identifiable personal data.

Robust functionality for PHRs requires the ability to exchange their data with the parties providing health services to the patient – e.g., physicians in clinics, hospitals, pharmacies. Broad social acceptance of PHRs requires that these exchanges are appropriately protected. It is not irrational to prefer to keep information out of institutional records if one cannot control its use and it can be used in destructive ways – a rationality that applies to PHRs if that content will reappear in institutional backups.

Providing a strong consent model for PHRs is not without costs. The information in PHRs has value, for all the reasons that institutional health records have value. Making PHRs attractive from a personal privacy perspective trades off that value, albeit in ways extremely difficult to quantify. Discrimination and bias fears suggest the need for laws that contemplate broader anti-discrimination and access protections, similar to the Genetic Information Nondiscrimination Act (GINA) [9,10].

Social networking poses a great and continuing challenge regarding privacy and confidentiality. Online communities and internet service providers are not covered entities under HIPAA, and it is not at all clear whether they should receive such or similar legal coverage. But if not HIPAA or HIPAA-like protections, by what mechanism should the privacy of online community inhabitants be protected? [11].

7. Conclusion

Is a PHR best viewed as a complement to the official record – a nice thing to have, with greater or lesser value depending on the PHAs it supports? Or is a PHR a substitute for an official record – required in emergency situations (an electronic form of "medical alert bracelet") and perhaps even in routine ones as a backup to inter-operable, inter-institutional EMRs? How much reliance during a routine clinical encounter can (or should) a health practitioner place on the data within a person's PHR? Whatever the legal, professional and social answers to these questions, there are technical and cognitive constraints that limit what can be expected of the average individual.

There is also the question of whether PHRs are a niche product (for particular conditions/diseases) or a more general accessory that "everyone should have". While everyone ought to have a list of current medications, allergies, and major past illnesses – for themselves and for persons for whom they are responsible – that is a rather minimal collection of data. Given the uncertainties about how institutional PHR providers would use data, it is difficult in good conscience to recommend them to persons who have strong preferences for privacy, instead of a simple printed list on a piece of paper. The balance tilts towards PHRs for particular conditions or diseases – those that are chronic, complex and have hard-to-manage treatment regimes.

In general, the nine projects of Project HealthDesign have helped make clear that: (a) the novel ways health information can be shared and distributed in a PHR world pose significant risks to privacy and confidentiality; (b) patients themselves play an unprecedented role in helping to safeguard their own health information in this new world; and (c) future PHR design and development must take into account the health aspirations and social and economic fears of patients.

Conflict of interest statement

The authors declare that there are no conflicts of interest.

Acknowledgments

The authors thank the principal investigators and other team members from the nine Project HealthDesign phase one grantees for their critical insights into the ELSI issues presented by their own projects and those at other sites. We also thank the Robert Wood Johnson Foundation for its funding of the ELSI group to serve as advisors to the nine projects.

Appendix A. Project HealthDesign projects and some example ELSI issues

Phase one efforts included: inter-operable "transmedia" PHR systems for young adults; a portable PC to assist older patients in transitional care; a PHR focused on at-risk sedentary adults; an electronic health diary to record pain and activity data; a child-focused electronic medication manager; a PHR for those with diabetes to record and upload glucose levels and other diabetes-related indicators; a computerized "conversational assistant" to provide patients with heart disease with a "daily check up"; and an application to make individualized health recommendations to diabetes patients [12].

A.1. Privacy and confidentiality

A.1.1. Granular control over disclosure

Revelations from disclosures to inappropriate third parties can be as freighted as a diagnosis of a mental disorder or a sexually transmitted disease, or as seemingly innocuous as data about one's "lifestyle" behaviors that have health implications. One fitness-related PHR site raised concerns about inappropriately-disclosed information regarding sedentary lifestyles, because participants

feared penalties from insurers and employers attributing sedentary lifestyles to future maladies. Other concerning lifestyle disclosures included smoking, drinking and eating behaviors.

Project HealthDesign investigators reported that patients had clear and distinct preferences between health-related data to be shared with peers (e.g., illegal substance use) and providers (a narrower list). There are clear technological obstacles to configuring role- and person-based access control in institutional data systems. Such structuring poses serious challenges on human decision-making by both system designers and the ultimate system users. Pushing the decision burden back to the individual data subject, technology permitting, does not solve the problem if implementing such decisions exceeds the abilities (or inclinations) of the average PHR holder.

A.1.2. Ubiquitous monitoring

One test site proposed a tablet-based medication list coordination tool, which, when paired with a PHA database, becomes an extension of "ambient computing", such that a potentially large volume of data is collected. Some projects also proposed the use of ubiquitous sensors to monitor and report the patient's current condition and accordingly adjust medication.

Such concerns emerge even if the data sources are not high-tech. One site's PDA-based data "diary" included records of daily activities. Unlike the previous technological monitoring, this site's recording device is the patient himself. Self-reported data could include details of intimate behaviors, use and abuse of controlled substances and other sensitive topics material to one's mental and physical health status. Memorializing such sensitive information in a permanent record whose sharing may not be controllable presents an additional privacy problem.

A.1.3. Cohort effects and vulnerable populations

The sites' implementations of PHRs revealed disparities in expectations of privacy and technological competence by age cohort. Many Project HealthDesign investigators reported that children and the elderly patients voiced fewer privacy concerns related to the consequences of disclosing health information. Pediatric patients were more willing, even eager, to share personal health data. This attitude, combined with greater technical familiarity with computing devices, seems to produce the unsurprising result that younger patients are more willing to enter all the required data to complete a robust PHR and share this data. The elderly patients seemed concerned more about treatment efficacy than nuances of privacy.

The appropriate range of actions by persons outside the parent–child dyad, such as non-parent family members, and by parties outside the family, was raised by other projects. Some sites' PHR implementations were explicitly designed to operate within a school setting, leading to questions about data protection obligations of school authorities, particularly in public school settings.

A.1.4. Social networking

Several projects made clear that social data sharing embeds varying views regarding the scope of privacy expectations. Youthful participants in one Project HealthDesign project were found to have stratified privacy zones that were far more detailed than those of other age groups. Some participants regarded privacy as incompatible with authenticity. Such disparities are hard enough to manage in adults; with unemancipated minors the appropriate overlay of controls by a parent or guardian becomes extraordinarily difficult.

A.2. Data security

Individual Project HealthDesign sites raised particular technical questions by virtue of the specific equipment employed, particularly the range of portable devices. Devices included cell phones, portable computers, portable sensors and USB storage devices.

A.3. Decision support

No site proposed a simple PHR consisting solely of static health data. All included some sort of PHA, the information from which provided varying levels of decision support. One Project HealthDesign site included very ambitious decision support functionality related to care-planning. Another used a PHR-based "personal assistant" involving natural language processing and decision support for "intention recognition", which could be of nontrivial significance in disease management. Another site, using multiple sources for monitoring data, incorporated some automated responses to data uploads, raising questions of entry error, notice/warning triggers, among others.

One site's interactive care-planning tool provided decision support for long-term, multi-stage treatment choices, including both modalities and timing. By offering information and predictions for treatment timelines and answering queries, such as "how many treatments do I need" and "will I be able to go on the long-planned family vacation", the types of decision support are varied and touch on social concerns as well as medical decisions.

One site proposed a medication–reconciliation and scheduling system that would be semantically linked to authoritative texts – a kind of "electronic pill box" from which dispensing behaviors would be triggered. Another Project HealthDesign project reminded pediatric patients when to take their medications and proposed to incorporate automatic drug dispensing from devices dressed up as toys. In this case, the especially vulnerable population for whom the PHR is targeted raised particular questions about parental competency and "fail-safe" measures. Investigators reported that some participants feared repercussions from insurers if it were found they failed to follow automated recommendations.

A.4. Legal-regulatory requirements

Current efforts to revise HIPAA under the auspices of the HITECH present an opportunity to address PHR issues. HITECH offers significant incentives for health care participants to adopt "meaningful use" of EMR technology, and every major vendor's implementation of EMRs offers a PHR component. The privacy and security elements of HITECH also focus on concerns implicit in wider electronic health data exchange, requiring: an audit trail of disclosure, notification of any breaches, additional authorization for certain uses of identifiable data, and strengthened enforcement of the federal privacy and security rules. HITECH specifically extends some of these HIPAA requirements to PHRs, treating them like "business associates" of entities covered by the law directly. But expanding the conception of business associates' or vendors' responsibilities in an EMR-like context only begins to meet PHR concerns. It extends an institutional model that only partly fits the world of PHRs and PHAs.

References

[1] American Health Information Management Association and American Medical Informatics Association. Joint position statement for consumers of health care: the value of personal health records. Available at <http://www.amia.org/files/ahima-amiaphrstatement.pdf>; 2007 [accessed 14.04.10].
[2] American Health Information Management Association, MyPHR. Site at <http://myphr.com/> [accessed 14.04.10].
[3] Project HealthDesign. Overview at <http://www.projecthealthdesign.org/about/overview> [accessed 14.04.10].
[4] American Medical Informatics Association (AMIA). ELSI Resources. Available at <http://www.amia.org/elsi-wg/elsi-resources> [accessed 14.04.10].
[5] Markle Foundation. Connecting Consumers: Common Framework for Networked Personal Health Information at <http://www.connectingforhealth.org/phti/> [accessed 14.04.10].

[6] National Committee on Vital and Health Statistics of the US Department of Health and Human Services. Enhanced protections for uses of health data: a stewardship framework for "Secondary Uses" of electronically collected and transmitted health data. Available at <http://www.ncvhs.hhs.gov071221lt.pdf>; 2007 [accessed 14.04.10].
[7] American Recovery and Reinvestment Act of 2009 (ARRA, a.k.a., "the Stimulus Bill"). Public Law No. 111-5, Title XIII, subtitle Health Information Technology for Economic and Clinical Health Act (HITECH Act), Sections 13401ff; 2009.
[8] Health Insurance Portability and Accountability Act (HIPAA) of 1996. Public Law No. 104-191; 1996.
[9] Genetic Information Nondiscrimination Act (GINA) of 2008. Public Law No. 110-233; 2008.
[10] Hudson KL, Holohan MK, Collins FS. Keeping pace with the times – the genetic information nondiscrimination act of 2008. New Engl J Med 358 (2008) 2661–3. Available at <http://content.nejm.org/cgi/content/full/358/25/2661> [accessed 14.04.10].
[11] Abril PS, Cava A. Health privacy in a techno-social world: a cyber-patient's bill of rights. New J Tech Intell Prop 6 (2008) 244. Available at <http://www.law.northwestern.edu/journals/njtip/v6/n3/1/> [accessed 14.04.10].
[12] Project HealthDesign, 2006–2008 Projects, <http://www.projecthealthdesign.org/projects/overview-2006_2008> [accessed 14.04.10].