11-13-2009

A Privacy Framework for Mobile Health and Home-Care Systems

David Kotz
Dartmouth College

Sasikanth Avancha
Intel Labs Bangalore

Amit Baxi
Intel Labs Bangalore

Recommended Citation
David Kotz, Sasikanth Avancha, and Amit Baxi. A privacy framework for mobile health and home-care systems. In Workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS), November 2009. 10.1145/1655084.1655086

A Privacy Framework for Mobile Health and Home-Care Systems

David Kotz
Computer Science; ISTS
Dartmouth College
Hanover, NH, USA

Sasikanth Avancha
Systems Research India
Intel Labs Bangalore
Bangalore, India

Amit Baxi
Health Systems Research
Intel Labs Bangalore
Bangalore, India

ABSTRACT

In this paper, we consider the challenge of preserving patient privacy in the context of mobile healthcare and home-care systems, that is, the use of mobile computing and communications technologies in the delivery of healthcare or the provision of at-home medical care and assisted living. This paper makes three primary contributions. First, we compare existing privacy frameworks, identifying key differences and shortcomings. Second, we identify a privacy framework for mobile healthcare and home-care systems. Third, we extract a set of privacy properties intended for use by those who design systems and applications for mobile healthcare and home-care systems, linking them back to the privacy principles. Finally, we list several important research questions that the community should address. We hope that the privacy framework in this paper can help to guide the researchers and developers in this community, and that the privacy properties provide a concrete foundation for privacy-sensitive systems and applications for mobile healthcare and home-care systems.

Categories and Subject Descriptors

A.1 [**General**]: Introductory and Survey; J.3 [**Computer Applications**]: Life and Medical Sciences—*Medical Information Systems, Health*; K.4.1 [**Computers and Society**]: Public Policy Issues—*Privacy*

General Terms

Security, Legal Aspects, Human Factors

Keywords

privacy framework, medicine, electronic health record, home healthcare, mobile healthcare, mhealth, e-health, HIPAA

Acknowledgements

Supported by Intel Corporation and by NSF Trustworthy Computing award 0910842. Thanks also to the reviewers.

SPIMACS'09, November 13, 2009, Chicago, Illinois, USA.

1. INTRODUCTION

Healthcare information technology (IT) has huge potential to improve healthcare quality, improve efficiency, and reduce cost, and is currently on the cusp of major innovations and widespread deployment in the US and elsewhere.

In this paper, we specifically examine the role of *mobile* computing and communications technologies. Such **mHealth** technology [25] appears promising in many ways: enabling physicians to remotely monitor their patients' health and improve the quality of healthcare, enabling patients to manage their health more easily, enabling home-care providers to provide better quality at-home medical care to elders and reducing the cost of care by allowing patients to spend more time out of the hospital. Furthermore, the UN Foundation has recently formed the *mHealth Alliance* specifically to explore and promote the value of mobile computing technologies in improving healthcare in developing nations [35].

In mHealth, personal mobile devices (such as smart phones) accompanied by wearable, portable, and even embeddable sensors, will enable long-term continuous medical monitoring [5, 21, 36] for many purposes: for outpatients with chronic medical conditions (such as diabetes), individuals seeking to change behavior (such as losing weight), physicians needing to quantify and detect behavioral aberrations for early diagnosis (such as depression), home-care providers needing to track movements of elders under their care in order to respond quickly to emergencies (e.g., an elder may have fallen down) or athletes wishing to monitor their condition and performance. In this paper, we use the term "Patient" to describe the subject of sensing in all such use cases. We expect that tomorrow's personal mobile devices will contain the technology and applications needed to process sensor data and enable their appropriate use. The resulting data may be used directly by the Patient [1, 2, 37] or may be shared with others: with a physician for treatment [33], with an insurance company for coverage, with a home-care provider for elder-care, with a scientist for research [12, 30], with a coach for athletic training [4], or with family members and friends in social-networking communities targeted towards health and wellness.

Although mHealth systems have huge potential to improve quality of healthcare and to improve quality of life, they also generate new security and privacy issues [23]. The technology goal should be to develop *usable* devices that respect patient *privacy* while also retaining the data *quality* and *accessibility* required for the medical uses of the data. In this paper, we focus on privacy; specifically, we wish to give the patient control over the data that is collected and

to whom it is disclosed, and enable the patient to recognize that different situations may require different responses. Indeed, we note that *control*, not possession or ownership, is fundamental to privacy. Privacy means that the patient retains some control even when the data is "owned" by another party (as is common in medical records maintained by a hospital) and even after a copy of the data has been provided to another party (as when billing records are shared with an insurance company). Security issues generated by mHealth systems are beyond the scope of this paper.

Although the term "mHealth" applies broadly to the use of mobile technology in healthcare applications, we focus here on patient-centered technology, as described in the examples above. There are, of course, valuable uses of mobile technology in other aspects of healthcare delivery and management, including personal digital assistants (and personal communication devices) used by clinicians, inventory-control systems for medical equipment and consumables, and telemedicine platforms for emergency response or remote rural healthcare. Although these mHealth applications also involve security and privacy issues, we do not address them here.

This paper makes four primary contributions. First, we compare existing privacy frameworks, with an eye to mobile healthcare and home-care systems (Section 3). Second, we identify a conceptual privacy framework – a set of actionable privacy principles – for mHealth (Section 4). Third, we extract a set of privacy properties intended for use by those who design systems and applications for mobile healthcare and home-care systems (Section 5), and demonstrate their application to a case study. Finally, Section 7 lists several key research questions for the community.

2. BACKGROUND

Before we discuss the existing privacy frameworks, we define "privacy" in the context of healthcare, and we lay out an abstract architecture for mHealth systems, to provide a foundation for the discussion ahead.

Privacy.

Given our focus on privacy, it is essential that we define it clearly for the context of healthcare. Fortunately, others have thought deeply about this issue; we adopt the definition selected by the National Committee for Vital and Health Statistics (NCVHS), a key advisory committee to the US Department of Health and Human Services. "*Health information privacy* is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data. *Confidentiality*, which is closely related, refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate. *Security* is altogether different. It refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure" [11]. We also follow NCVHS and define PHI as "personal health information" rather than "protected health information", which is a phrase that has specific meaning in a HIPAA context [10].

Clearly, privacy is important in any healthcare information system. What is different, or especially challenging about *mHealth* privacy? First, mHealth allows for the collection of far more medical data about the Patient, as many mHealth devices collect data continuously over extended periods of time. Second, mHealth allows much broader range of *health* information to be collected, not just *medical* information: in addition to collecting physiological data, many mHealth applications will collect information about Patient lifestyle and activities (such as food habits and diet details, location tracks, physical activity, or social interactions). Third, mHealth will enable a broad range of health-related applications: sharing data with your health provider, as in a traditional doctor relationship, but also sharing data with an insurance company (e.g., to confirm compliance with a medicine regimen), with lifestyle coaches (e.g., diet advisers), with athletic coaches (e.g., sports teams or health-club trainers), with a home-care provider (e.g., to care for an elderly person) or with family (e.g., to support a relative's recovery from surgery). In such settings, privacy is a complex issue: the Patient needs subtle control over the collection, recording, dissemination, and access to their mHealth data.

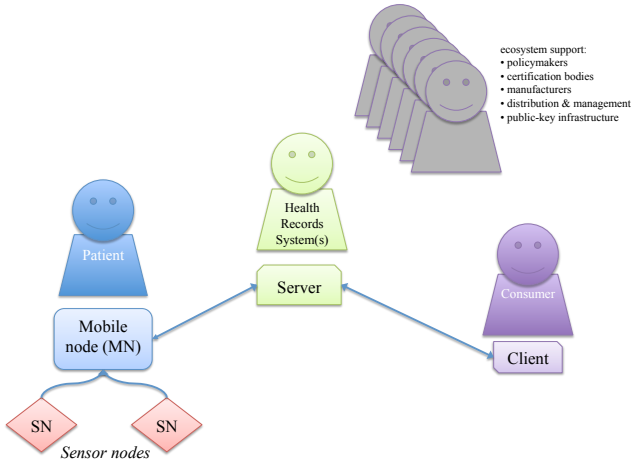

Figure 1: mHealth Reference Architecture

Architectural model.

Figure 1 portrays a high-level view of the structure and context of patient-centric mHealth deployments. We imagine an infrastructure in which each Patient carries a mobile node (MN), which may be their mobile phone or other mobile Internet device (MID), and a personal collection of sensor nodes (SNs) that can measure data about their activity (accelerometers, pedometers, GPS) or physiology (electrocardiograms, pulse oximeters, blood-glucose meters, weight scales). These sensors may be carried by the patient [22], worn by the patient [29], embedded in their living space [33], or implanted in their body [13]. The sensors communicate with the MN through a body-area network. The MN is responsible for coordinating the sensors, collecting the sensor data, (optionally) aggregating or pre-processing the sensor data, and reporting the data to a health records system (HRS). The MN also serves as the Patient's primary interface to the HRS, with respect to managing the data-collection process and subsequent sharing of the data.

The health records system (HRS) may be a Personal Health Record (PHR) or Electronic Health Record (EHR) system; most of the mobile-centric research challenges will be the same for both scenarios. We must also consider the likely situation, over the next decade, in which a Patient must interact with multiple health-records systems from multiple providers and built on different models.

The Consumers of these records, including doctors and other clinical personnel, insurance companies and other billing-related personnel, researchers and regulators, access the HRS through some Client computer. The security issues on this platform are largely out of scope of this paper, except in cases where we seek end-to-end technical mechanisms to support the Patient's privacy wishes.

Finally, these people and systems need a supportive ecosystem, a set of authorities and agencies that provide the regulatory, logistical, and technical foundation for the above relationships. We can identify at least five roles to be played by some combination of public and private organizations:

- **Policymakers** establish laws, regulations, and standards regarding the protection of Patient privacy in mHealth technology.
- **Certification bodies** attest to whether particular products and services meet the policies and standards.
- **Manufacturers** produce hardware and software products and services, such as the MNs, SNs, and HRS.
- **Distribution & management** services distribute the hardware and software to Patients and Consumers, and provide remote-management capabilities such as secure, automatic software updates and remote deletion of data and keys on lost devices.
- **Public-key infrastructure** provides the key-distribution and certificate authorities to support the crypto-systems used for verification (e.g., to verify the signature of a certification body regarding an SN calibration, or to verify the public key of a management service).

We should take care not to expect that a top-down definition of, let alone deployment of, such an infrastructure is possible. Any such system will necessarily be defined and deployed by many organizations and agencies, over time [32].

In the above infrastructure we expect that the Patient would use their personal device as an MN; although the use of a such a device is expedient, because the patient already owns such a device and wants to carry it for other purposes, there are many risks: the sensor data may be intercepted (impacting privacy), tampered with (leading to improper care decisions), or blocked (leading to loss of critical information to researchers or care providers). Furthermore, MNs or SNs may be lost or stolen, resulting in possible exposure of any data or encryption keys they contain. All of these risks can lead to dangerous consequences for the patient and provider [20, 34].

Although any viable solution, and any real deployment, will doubtless be more complex than implied by this figure, this architecture provides a structural basis and terminology for our discussion of privacy frameworks and privacy properties, below.

3. CONCEPTUAL PRIVACY FRAMEWORKS

Given the above definition for health information privacy, then, we define a *conceptual privacy framework* to be a coherent set of actionable principles to protect patients' health information privacy. When developing and deploying a healthcare information system, the system design should include security and privacy properties that align with the principles in the conceptual privacy framework.

Although major laws (notably HIPAA [14] and ARRA [9]) provide a legal foundation for healthcare privacy, at least in the US, these laws provide few details. Thus, others have set out to define conceptual privacy frameworks, privacy principles, or best practices for privacy, in the healthcare context. In this section, we summarize the frameworks proposed by the US Office of the National Coordinator (ONC), the Health Privacy Project, the Markle Foundation, and the Certification Commission for Healthcare Information Technology (CCHIT).

3.1 ONC National Framework (2008)

In December 2008 the Office of the National Coordinator for Health Information Technology (in the US Department of Health and Human Services) released an important report, announcing its *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information* [28]. This document, which we call the "ONC Framework", provides the newest and most authoritative privacy framework for healthcare released in the US, so we present it first. We quote their eight principles as follows, adding numbers for ease of reference within this document. Their document includes additional explanatory detail that we do not quote here.

ONC1. **INDIVIDUAL ACCESS.** Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.

ONC2. **CORRECTION.** Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied.

ONC3. **OPENNESS AND TRANSPARENCY.** There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information.

ONC4. **INDIVIDUAL CHOICE.** Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information.

ONC5. **COLLECTION, USE, AND DISCLOSURE LIMITATION.** Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.

ONC6. **DATA QUALITY AND INTEGRITY.** Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.

ONC7. **SAFEGUARDS.** Individually identifiable health information should be protected with reasonable

administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.

ONC8. **ACCOUNTABILITY.** These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate nonadherence and breaches.

We next consider some important predecessors and inspirations for the ONC Framework, in chronological order.

3.2 HPP best principles (1999)

The Health Privacy Working Group, organized by the Health Privacy Project, released a set of "best principles" for health privacy in 1999 [15]. The document, which we call the "HPP Framework", notes that their "principles are intended to establish a comprehensive framework". We quote their 11 principles as follows; note that their report provides additional depth beyond these high-level statements.

HPP1. For all uses and disclosures of health information, health care organizations should remove personal identifiers to the fullest extent possible, consistent with maintaining the usefulness of the information.

HPP2. Privacy protections should follow the data.

HPP3. An individual should have the right to access his or her own health information and the right to supplement such information.

HPP4. Individuals should be given notice about the use and disclosure of their health information and their rights with regard to that information.

HPP5. Health care organizations should implement security safeguards for the storage, use, and disclosure of health information.

HPP6. Personally identifiable health information should not be disclosed without patient authorization, except in limited circumstances. Health care organizations should provide patients with certain choices about the use and disclosure of their health information.

HPP7. Health care organizations should establish policies and review procedures regarding the collection, use, and disclosure of health information.

HPP8. Health care organizations should use an objective and balanced process to review the use and disclosure of personally identifiable health information for research.

HPP9. Health care organizations should not disclose personally identifiable health information to law enforcement officials, absent a compulsory legal process, such as a warrant or court order.

HPP10. Health privacy protections should be implemented in such a way as to enhance existing laws prohibiting discrimination.

HPP11. Strong and effective remedies for violations of privacy protections should be established.

Many of these themes resonate in the ONC Framework, but we want to call attention to HPP2 and its underlying detail, which notes that "All recipients of health information should be bound by all the protections and limitations attached to the data at the initial point of collection". This transitive application of privacy constraints does not explicitly appear in the ONC principles, but we believe it is an important feature and deserves its top-level appearance in the HPP Framework. (This principle shows up again as BP6, below.) We anticipate that there may interesting methods for technological protection of PHI, wrapping any PHI with privacy policies before sharing with a third party.

3.3 HPP best practices (2007)

The Health Privacy Project recently listed 10 "best practices" for employers who are developing personal health records (PHR) [16]. We quote their list as follows, adding numbers for reference.

BP1. **Transparency and notice.** Employers should be transparent about their reasons for offering a PHR to employees and all policies that apply to the PHR. Employers should provide an Information Policy Statement or Notice that clearly lays out the ways in which information in the PHR will be used and safeguarded. Employers should incorporate the Notice into their health benefit programs, and should make it available in a layered format a short concise version to accompany a more detailed one. Employees should be informed of any updates to the policy.

BP2. **Education.** Employees should be educated about the benefits, functions, and content of the PHR. Information about the PHR should be communicated in numerous ways to build both knowledge and trust.

BP3. **Employees can choose which content is included in the PHR.** Employees should be able to determine the content of the PHR, including which providers and plans contribute to it. Employees should be able to annotate the records submitted by others, as well as to enter their own information, with employee-entered data marked as such. The identification of sources of all personal health information in the PHR should be readily apparent.

BP4. **Employees control access to and use of the PHR.** A. Employees should control who is allowed to access their PHRs. Employers should not access or use employees' individually-identifiable health information from the PHR. B. Employees should choose, without condition, whether to grant access to personal health information within their PHRs for any "secondary uses". An audit trail that shows who has accessed the PHR should be easily available to employees.

BP5. **Employees can designate proxies to act on their behalf.** Employees should determine who,

including family members and caregivers, should have direct access to their PHRs on their behalf. Where possible, employees should be able to grant proxy access to full or partial information in their PHRs, including access in emergency circumstances. Employees should also have the ability to revoke access privileges.

BP6. **"Chain of trust": Information policies extend to business partners.** The information policies and practices of employer-sponsored PHRs should follow the data through chain of trust agreements that require business partners to adhere to the employer's applicable policies and practices.

BP7. **Data security.** Employers should provide a strong level of security to safeguard the information in the PHR systems. A robust authentication process for access to PHRs should be required, in addition to an audit trail that shows who has accessed information and when.

BP8. **Data management.** Employers should ensure that the PHR systems they provide have comprehensive data management strategies that protect the integrity of the data and include data retention policies.

BP9. **Enforcement and remedies.** Employers should establish oversight and accountability mechanisms for adhering to their PHR policies and practices. Employers should put into place a mechanism to promptly notify employees of any inappropriate access to or use of information contained in an employee's PHR, identify the steps which have been taken to address the inappropriate activity, and make resources available to employees to assist them in addressing the effects of the inappropriate activity.

BP10. **Portability.** Employers should offer PHRs that are portable, to the extent feasible, allowing employees to maintain or move the PHR and/or the data it contains even after employment or coverage ends or changes.

We note that the ONC Framework largely covers these practices. There are some aspects specific to PHR systems, such as Patient-entered data (BP3) and portability (BP10). There are some aspects specific to employer-provided systems, such as Education (BP2). BP5 mentions the concept of a "proxy", which is not mentioned by any of the other frameworks, except ONC4 (in the details). The "chain of trust" concept (BP6) is more explicit than in any of the privacy frameworks, except the HPP's own earlier framework (see HPP2). There is explicit mention of the requirement to notify the Patient of any inappropriate disclosure (BP9); the ONC Framework only mentions such notice in its detailed comments, and only as an example of a reaction and not as a requirement. The Common Framework (below) mentions a similar requirement in its detailed comments about CF7.

3.4 Markle: Common Framework (2008)

The Markle Foundation launched a project "Connecting for Health", which brought together a wide range of stakeholders in developing a "Common Framework", a model for healthcare information exchange [24]. The Common Framework (CF) describes both policy and technical principles for healthcare information exchange, and provides concrete prototypes of each: everything from patient consent forms to data-interchange formats and information architecture. The Center for Democracy & Technology later endorsed the policy aspects of the Common Framework in their own policy document [8]. We quote the top-level description of the CF principles here.

CF1. **Openness and transparency:** Consumers should be able to know what information has been collected about them, the purpose of its use, who can access and use it, and where it resides. They should also be informed about how they may obtain access to information collected about them and how they may control who has access to it.

CF2. **Purpose specification:** The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes, or others that are specified on each occasion of change of purpose.

CF3. **Collection limitation and data minimization:** Personal health information should only be collected for specified purposes and should be obtained by lawful and fair means. The collection and storage of personal health data should be limited to that information necessary to carry out the specified purpose. Where possible, consumers should have the knowledge of or provide consent for collection of their personal health information.

CF4. **Use limitation:** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.

CF5. **Individual participation and control:** Consumers should be able to control access to their personal information. They should know who is storing what information on them, and how that information is being used. They should also be able to review the way their information is being used or stored.

CF6. **Data quality and integrity:** All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and up-to-date.

CF7. **Security safeguards and controls:** Reasonable safeguards should protect personal data against such risks as loss or unauthorized access, use, destruction, modification, or disclosure.

CF8. **Accountability and oversight:** Entities in control of personal health information must be held accountable for implementing these principles.

CF9. **Remedies:** Remedies must exist to address security breaches or privacy violations.

The ONC Framework covers all these principles. CF1 is covered by ONC3 (Openness and transparency), and ONC1

(Individual access). CF2 is covered by ONC5 (Collection, use, and disclosure notification) and ONC1. CF3 is covered by ONC5 and ONC4 (Individual choice). CF4 is covered by ONC5. CF5 is covered by ONC1 and ONC4. CF6 is covered by ONC6 (Data quality and integrity). CF7 is covered by ONC7 (Safeguards). CF8 is covered by ONC8 (Accountability). CF9 is covered by ONC8 and ONC2 (Correction).

Furthermore, we see little in the ONC principles that is not covered in the Common Framework, except that ONC1 provides more explicit statement that Patients should have an easy method to obtain their PHI, ONC2 provides an explicit statement that Patients should be able to correct mistakes in their records, ONC3 explicitly states openness about policies and technologies, and ONC4 emphasizes that Patients should be able to make informed choices.

[As an aside, we note that it may be difficult to decide how and whether to provide Patients with the capability to edit, annotate, and delete PHI in their record. The right policy depends on the type of record; a PHR, for example, allows a Patient to upload their own PHI, may allow them to annotate PHI give by a healthcare provider, and may allow them to delete data they have entered or whole sections of data (e.g., all the data from a given provider). An EHR, however, forms part of the official records of a healthcare organization and must necessarily be more strict. A Patient might request annotations or even deletions; such changes would be subject to provider approval and be marked as Patient-initiated; 'deleted' data may be retained for recovery under certain override conditions (such as an audit). The "right" policies are a delicate balance of Patient rights, legal limits, and provider operational necessities. In general, our position is that providers should honor such requests unless there is a good reason not to do so.]

In a few cases, the ONC framework allows more flexibility, suggesting rather than requiring. For example, CF5 bluntly states that "consumers should be able to control access to their personal information"; ONC4 (individual choice) allows significant flexibility, only requiring that "individuals should be provided a reasonable opportunity" for choice, and (in the details) that "the degree of choice available may vary. . . ".

We believe that the Common Framework is a crisper statement of the important principles; it is also more explicit in emphasizing that data should be used only for the purpose for which it was collected, and that Patients should have control over what is collected and to whom the data may be disclosed.

3.5 CCHIT's certification criteria (2008)

The Certification Commission for Healthcare Information Technology (CCHIT) is a non-profit organization that certifies healthcare information systems, and they recently released their certification criteria for PHRs. Although it appears that they have a process in place to determine these criteria, and that the process may enable and encourage updates to the criteria, we quote the current list of criteria as published in a booklet copyrighted in 2008 [7].

CCHIT1. **Consent.** You should be in control of your personal health information and how it is used. PHRs that meet certification requirements must include safeguards that require you to give your explicit consent before your account is opened, or allow you to opt out of the service. It also must allow you to decide if your data can be collected, displayed, accessed, stored, released or disclosed.

CCHIT2. **Controlling Access to your Information.** Your PHR should give you the ability to decide what information is private and to restrict access to it. Your PHR provider must get your permission to gather or disseminate any information about you. You also decide who else can view information in your PHR, and limit the types of information that can be viewed.

CCHIT3. **Conditions of Use.** The conditions for using your PHR should be explicitly explained to you, and you have the right to challenge your PHR provider if it does not comply with the conditions of use. If conditions of use are changed, your PHR provider is required to notify you of the changes.

CCHIT4. **Amending the Record.** You should have the ability to change or request changes to your health record via email or telephone, and the telephone number of customer service must be posted on the Web site of your PHR provider.

CCHIT5. **Account Management.** Your PHR provider must have a way for you to terminate your account, if you wish, and to confirm that all your personal data has been deleted from the system.

CCHIT6. **Document Import.** Your PHR system should be able to retrieve health records, explicitly label and manage your personal health information and be able to distinguish between data entered by you and data retrieved from other sources.

CCHIT7. **Data Availability.** Your system should allow you to view or print your health information whenever you need it.

It is instructive to compare these criteria with the HPP Best Practices for PHR systems, since both attempt to cover the same ground. CCHIT1 (consent) is covered by BP3 (choose which content), BP4 (control access), and BP1 (transparency). CCHIT2 (control) is similar to BP4 (control). CCHIT3 (conditions of use) is similar to BP1 (transparency and notice). CCHIT4 (amending) is mentioned by BP3, although BP3 calls it "annotating" rather than "amending", which in some contexts may be an important difference. CCHIT5 (the ability to delete your account) is not covered by any HPP Best Practice, which is an interesting omission. CCHIT6 (document import) is about capability (ability to import documents) and about distinguishing user-entered data from provider data (which is mentioned by BP3). CCHIT7 (availability) is not covered by any HPP Best Practice, even BP8 (data management).

There are many of HPP's Best Practices that do not appear in the CCHIT criteria. In particular, BP1 is more specific than CCHIT3 about the presentation and quality of the terms and notification, BP2 (education of the user) is not covered, BP3 is more clear that sources of data should be clearly identified, BP4 precludes employer use of employee PHR data, BP4 requires an audit trail and that the audit trail be easily available, BP5 allows the designation of proxies, BP6 requires the "chain of trust" in which privacy

policies follow the data to other business partners, BP7 requires strong mechanisms for security, access control, and access logs, BP8 requires data-integrity policies and mechanisms, BP9 requires notice and assistance in the event of a data breach, and BP10 requires PHR portability to new employers. None of these aspects – many of which we believe are important properties – are covered by the CCHIT criteria, leading us to the opinion that the CCHIT Criteria are too weak and should be strengthened.

Similarly, the CCHIT criteria fall short of the ONC framework. ON3 (openness and transparency) is covered somewhat by CCHIT3 (conditions of use), but not the requirement (stated in the details) for access to an audit log. ONC4 (individual choice) says (in the details) that a Patient should be able to designate a proxy, which is not mentioned in the Criteria. ONC5 (collection, use, and disclosure) limits the collection, use, and disclosure of PHI to the minimum necessary for a particular purpose and the Criteria have no such concept; of course, a PHR is intended to collect PHI more widely than an EHR, at the discretion of the Patient, but this concept should still apply to the disclosure and use of PHR information. ONC6 (data quality and integrity) states the obligation of providers to ensure records are complete and correct; no such requirement appears in the Criteria. ONC7 (safeguards) describes security and data-integrity requirements, which do not appear in the Criteria. Although CCHIT1 says the Patient should be able to challenge the PHR provider if they do not follow their terms of use, the Criteria have nothing like ONC8 (accountability) that requires the PHR provider to have mechanisms for monitoring internal compliance, and for notifying Patients if there is a data breach. Again, it is our opinion that the CCHIT Criteria are too weak and should be strengthened.

3.6 Others

We have insufficient space here to describe in depth all of the relevant privacy frameworks.

We note with interest an earlier, detailed survey of privacy principles for healthcare, by Buckovich et al. [6]. Although interesting, this 1998 survey pre-dates all of the documents we survey here, even pre-dating HIPAA.

The Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [27] is an old list of eight principles that, although not specific to healthcare, has inspired all of the above frameworks.

The Asia-Pacific Economic Community (APEC) published a privacy framework, a set of "information privacy principles", in 2005 [3]. This framework is not specific to healthcare, and is meant more generally for the commercial use of personal information. One analyst, however, shows that there are too few details – and far too much flexibility – in the APEC Framework for it to be useful [31].

The International Security, Trust, and Privacy Alliance conducted a 2007 analysis and comparison of several important privacy frameworks from around the world [18]. The committee that developed the ONC Framework considered this document in their work. Although not specific to healthcare, this document is helpful because it brings a broad, international perspective to privacy frameworks, and attempts to provide uniform definitions for common terms. Although their final list of definitions are not a set of principles, implicit in these terms are the core concepts of many privacy principles. These definitions build on their earlier work, a Privacy Framework [17], although that document is mostly focused on an architecture for "services and capabilities" in handling personal information throughout its life cycle. It does little, specifically, to generate a precise set of principles.

The Health Information Trust Alliance (HITRUST) released a security framework for healthcare in March 2009, but it is available only to member organizations and only for a fee [19]. Little information is available about this framework and it is not clear whether it includes a comprehensive set of privacy principles.

4. AN MHEALTH PRIVACY FRAMEWORK

So, after reviewing all those conceptual privacy frameworks, which one do we recommend as the basis for research and development in mHealth systems? Both the ONC Framework and the Common Framework (CF) are appealing, because both are recent (2008), both are fairly complete, and both were developed by diverse groups of experts and stakeholders. We chose to use the Common Framework for four main reasons.

First, the CF more clearly states the fundamental privacy principles for healthcare information systems. The ONC Framework leaves many important issues to the details, rather than expressing them in the main bullets. Indeed, the ONC Framework leaves certain issues implicit. When privacy is at stake, it is important to be explicit. Second, the ONC Framework is less concrete, leaving flexibility on several principles. We believe it is important to state the core principles, clearly and simply, and to aim implementations at them. Third, the CF has a more Patient-centric viewpoint. Finally, concrete materials accompany the CF principles: everything from patient consent forms to data-interchange formats and information architecture.

We restate CF principles for completeness.

CF1. **Openness and transparency**

CF2. **Purpose specification**

CF3. **Collection limitation and data minimization**

CF4. **Use limitation**

CF5. **Individual participation and control**

CF6. **Data quality and integrity**

CF7. **Security safeguards and controls**

CF8. **Accountability and oversight**

CF9. **Remedies**

We cannot resist the temptation to incorporate a few important principles best described by other frameworks:

- From BP3: Patients "should be able to annotate the records submitted by others, as well as to enter their own information, with employee-entered data marked as such."
- From BP5: Patients "can designate proxies to act on their behalf. [Patients] should determine who, including family members and caregivers, should have direct

access to their PHRs on their behalf. Where possible, [Patients] should be able to grant proxy access to full or partial information in their PHRs, including access in emergency circumstances. [Patients] should also have the ability to revoke access privileges."

- From BP6: "The information policies and practices... should follow the data through chain of trust agreements that require business partners to adhere to the... applicable policies and practices."
- From ONC1: Patients should have an easy method to obtain their PHI in a readable electronic format.
- From ONC2: Patients should be able to correct mistakes in their records.
- From ONC3: The system should be open about the policies and technologies in use.
- From ONC4: Patients should be able to make informed choices about what data is collected, how it is used, and to whom it is disclosed.
- New: the presence of medical sensing devices, or of sensor-data collection, should not be observable by nearby parties (this privacy threat is unique to mHealth).

In summary, there are several existing conceptual privacy frameworks. Each has been developed by experts in the field, usually by large bodies of diverse stakeholders who have worked for months or years to examine relevant laws, documents, and current practices. Many of the above frameworks have been developed after studying the others, and thus there is a significant degree of overlap. On the other hand, there is a surprising degree of difference in the principles, and some frameworks have notable omissions. There is fairly broad agreement about general principles, but there is room for reasonable disagreement about the details, in part because there are difficult trade-offs between protecting privacy and providing efficient, effective healthcare. The NCVHS discussed several of these issues in 2006 [11], and revisited some of them in 2008 [26]. We chose the Common Framework (CF) as our own working framework for the purpose of research and development, albeit with some appendages drawn from some of the other frameworks.

5. PRIVACY PROPERTIES

A high-quality mHealth system should protect privacy and data integrity, remain available, and be auditable. We derive the following properties from the above privacy principles (as specified in parentheses below), and add the necessary integrity, availability, and auditability properties. (See Table 1 to cross-reference with the above frameworks.) Finally, we list the functional properties for completeness.

Security and privacy properties.

A high-quality mHealth system should:

P1. Inform patients (CF1, CF2, ONC1, ONC4)
  a. *What* PHI is collected and stored
  b. *Why* PHI is collected and stored
  c. *Where* PHI is stored and at which organization
  d. *Who* has access to their PHI, and under what circumstances
  e. *When* PHI collection purpose (why) changes or access (who) changes
  f. *How* their PHI is used
  g. About *risks* of data collection or disclosure
  h. About security *breaches* or PHI misuse

P2. Enable patients to review storage and use of their PHI (CF5)
  a. Review historical records of all information in property P1.

P3. Enable patients to control, through informed consent (CF1, CF3, CF5, ONC4, BP5),
  a. What PHI will be collected and stored, and in what contexts
  b. When PHI will be collected and stored (allowing patients to stop and restart data collection)
  c. Who will have access to their PHI (including Patient proxies), and in what context
  d. How their PHI may be used, and in what circumstances

P4a. Enable patients to access their PHI (CF1, ONC1, BP3).

P4b. Honor patients' requests to add, annotate, correct and delete their PHI (CF6, ONC2, BP3), where possible.

P5. Provide easy-to-use interfaces for all of the above, including clearly defined terms and a layered presentation that allows interested users to dig into the details.

P6. Limit collection and storage of PHI (CF3)
  a. As needed for specified purpose
  b. Per limitations of patient consent
  c. Using lawful and fair means

P7. Limit use and disclosure of PHI to those purposes previously specified and consented (CF4, CF7)
  a. Policies should follow PHI as it flows to other entities (BP6)

P8. Ensure quality of PHI (CF6)
  a. Ensure data freshness and accuracy when collected
  b. Ensure data integrity and completeness during transmission, processing, and storage
  c. Ensure authenticity of patient providing input or wearing sensor
  d. Ensure authenticity and quality of sensors

P9. Hide patient identity, sensor presence and data-collection activity from unauthorized observers

P10. Support accountability through robust mechanisms (CF8)
  a. Include audit logs for all access, addition, deletion, and modification of PHI (the MN, too, should log its actions with respect to collection, upload, and access to PHI, and pairing with SNs and other devices)

P11. Support mechanisms to remedy effects of security breaches or privacy violations (CF9)

Table 1: Comparison of our security and privacy properties with other major frameworks; a framework item is mentioned if it covers some, though not necessarily all, of our property.

	Property	ONC	HPP	BP	CF	CCHIT
P1	Inform patients	ONC1,3,4	HPP4,6	BP1	CF1, CF2	CCHIT3
P2	Review storage and use	ONC1	HPP3		CF5	
P3	Informed consent	ONC4	HPP4,6	BP5	CF1, CF3	CCHIT1,3
P4	Access, annotate, correct	ONC1, ONC2	HPP3	BP3	CF1, CF6	CCHIT4,5,6,7
P5	Usable interfaces	*other frameworks do not emphasize usability*				
P6	Limit collection and storage	ONC5	HPP6	BP3	CF3	CCHIT2
P7	Limit to specified purposes	ONC5	HPP2	BP4, BP6	CF4, CF7	
P8	Ensure quality	ONC6, ONC7		BP7, BP8	CF6, CF7	
P9	Hide from observers	*this property is specific to mHealth*				
P10	Accountability	ONC8		BP4	CF8	
P11	Remedies			BP9	CF9	
	not related to privacy		HPP1,8,9,10	BP2,BP10		

Functional properties.
A high-quality mHealth system should be:

P12. **Flexible**, supporting multiple types of data
   a. Streaming data, i.e., high-frequency, periodic data
   b. Event data, i.e., low-frequency aperiodic data
   c. Patient-entered data, using one or more modes of input

P13. **Scalable**, to large numbers of participants (Patients and Consumers) and devices (MNs, SNs)

P14. **Efficient**, particularly regarding resources on MN and SN (CPU, memory, bandwidth, energy)

P15. **Usable**
   a. Patient: physical usability of sensors, i.e., preserve wearable-ness
   b. Patient and provider: easy interfaces for data collection and access
   c. Physically challenged Patients: accessible interfaces for informed consent and control over PHI

P16. **Manageable**
   a. Ensure remote configurability and calibration of system components
   b. Ensure ability to remotely manage lifecycle of software and credentials in system despite having no control over OS and firmware updates of system machinery
   c. Enable easy provisioning and de-provisioning of health applications, tools and data

P17. **Available**, preventing loss of (or loss of access to) PHI
   a. At MN, data latency and risk of loss must balance against resource limitations

We recognize that there are many subtle and in many instances, challenging, aspects to supporting these properties in an mHealth system, and that many of these properties are not unique to mHealth. Some of these properties will require support on the SN and MN; others may be achieved only in the back-end servers (HRS) or the data consumer's system (Client). Careful study is needed, in the context of a system design, to identify which properties will need support on the mobile platform. For example, the interface designed to ensure property P1 on a mobile node must be highly user-friendly because of the limited viewing area on its screen; the interface may have to be multi-modal to convey information effectively to the patient. As another example, because mobile nodes are highly vulnerable to physical loss or theft, they must be remotely manageable; i.e., an administrative entity must be able to disable or lock the mobile node remotely and prevent patient data from being stolen.

6. CASE STUDY

Here we illustrate how some of the aforesaid properties can be realized in a "privacy aware" mHealth system.

Ravi is a diabetic who finds it difficult to manage his condition effectively, resulting in significant variation of his diurnal blood-glucose levels, and frequently elevated blood pressure and cholesterol levels. Ravi's doctor advises him to subscribe to a Diabetes Management Program offered by his hospital. As part of the program, Ravi wears a hospital-provided device that continuously monitors his activity level and calories burned. The device is designed as a wrist watch to improve usability and to prevent anyone in Ravi's vicinity from detecting that he is wearing it **(P9-hide sensor presence)**. Upon first use, the device records features of Ravi's pulse waveform (plethysmograph). Whenever Ravi takes the device off his wrist and wears it again, the device uses the plethysmograph as a biometric to authenticate him. As long as Ravi wears the device, it monitors his activity and wirelessly sends encrypted data to his smartphone.

Also as part of the program, Ravi's smartphone is provisioned with certified software and a set of cryptographic keys. Upon installation and setup, the software on the smartphone uses one or more of the keys to authenticate the wrist device. The software further verifies that the device is properly calibrated and un-tampered, thereby ensuring data quality and integrity **(P8-ensure quality of PHI)**. The software processes data it receives from the device and acquires other contextual information such as Ravi's location (using GPS or Wi-Fi localization), ambient audio (using a microphone), calendar schedule and time of the day. This data is used to infer social context (such as whether Ravi is at home or at the office, in conversation or alone). The software reminds Ravi to take his medication, alerts him to long periods of inactivity, encourages him to log diet information and tracks his daily goals of calorie intake and expenditure. The phone synchronizes data with Ravi's PHR server.

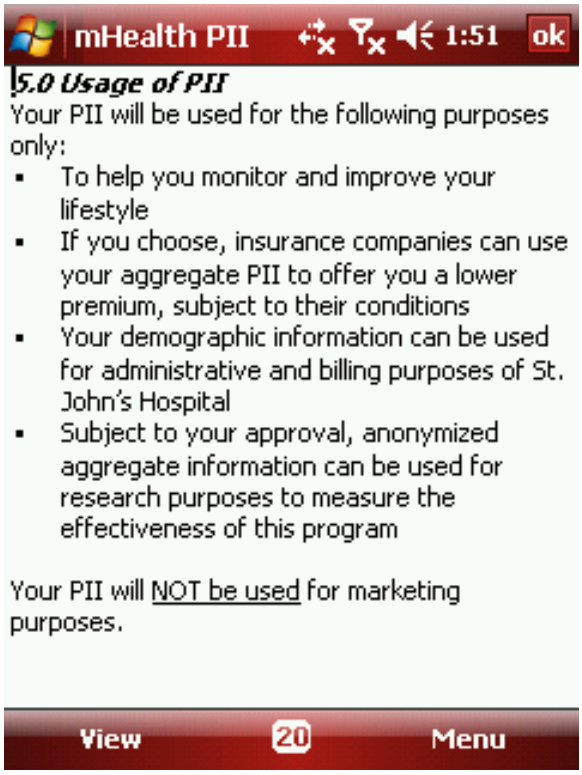

Figure 2: Screenshot of example policy

Before starting data collection, the smartphone application presents Ravi with a privacy policy; one screen of a sample policy is shown in Figure 2. Ravi observes that the privacy policy is easy to understand, clear and concise **(P5-easy to use interfaces)**, unlike verbose privacy policies on some health websites. The privacy policy clearly conveys **(P1-inform patients)** information about the collection, use, and storage of Ravi's Personally Identifiable Information (PII, a super-set of PHI).

After disclosing information about what PII will be collected and why, who has access to the PII and how it will be used, the software seeks Ravi's consent to begin using the system **(P3-informed consent)**. Specifically, the software presents Ravi options in the form of check boxes that allow him to control data collection and dissemination. It allows Ravi to control *data collection* by enabling him to specify times of the day during which data can be collected – by turning ON/OFF location sensing, audio sensing, and medical sensing **(P3-enable patient to control data collection and dissemination)**. It also allows Ravi to control *data dissemination* by specifying who (people, roles, or organizations) has access to his PHI and at what level of detail. Ravi allows detailed access to his PHI (including context) to his doctor and spouse, allows the insurance company access to his aggregate health trends, and allows researchers access to anonymized aggregate data only. Ravi also names his spouse as a "proxy", allowing her to act on his behalf and with all privileges equivalent to his. These steps are completed in the hospital under the supervision of an expert who can answer Ravi's questions about the privacy issues and policy interface, but Ravi can revisit this interface and change his preferences at any time.

An embedded accelerometer in the wrist device monitors Ravi's activity in terms on number of walking steps, and an optical sensor monitors his pulse rate (which is used to estimate exercise intensity). The system is able to accommodate real-time streaming data, periodic and aperiodic sampling of location information, audio and schedule; it also allows Ravi to manually enter diet information **(P12- flexible)**. A fusion algorithm on the smartphone estimates Ravi's context, which serves both to augment the medical data in the PHR and more immediately to provide customized and relevant reminders, tips, and motivational messages that encourage him to increase physical activity and control his diet. For example, when the smartphone determines that Ravi is running late for a meeting, it avoids prompting him to take the stairs instead of the elevator. Or, when the system determines that Ravi is in conversation, it avoids using spoken motivational messages.

Using authentication keys retrieved from a secure internal storage area, the smartphone periodically connects with the backend server to upload his activity, diet and context information, and to obtain messages for Ravi that arise from either automated or human analysis of his data. Ravi also receives a username and password for a secure web interface accessible from any computer **(P4-enable patients to access, add and annotate their PHI)**. The web interface presents detailed charts and trends of his health parameters, activity, diet information and established context, which help him to review, introspect and improve his lifestyle. Per Ravi's privacy choices, the same information is available to his spouse and doctor for review. However, the insurance company may only access high-level information about his fitness level. This is sufficient for the insurance company as Ravi's insurance premium depends on his fitness level.

Whenever Ravi is wearing the wrist device, he can seamlessly use his smartphone to view the backend-stored PII. When the wrist device is not present, or cannot biometrically verify Ravi as its wearer, the smartphone will only provide access to PII after entry of the password. This approach provides ease of use in the common case but prevents misuse in the case of device loss or device theft.

The backend server maintains audit logs **(P10-support accountability)** of all accesses, additions, and updates to Ravi's PII. With his password, Ravi can review at any time who has accessed which parts of his PII and when. The system also has mechanisms to send an alert SMS to Ravi's smartphone in case there is an unauthorized access to Ravi's PII or if there is a security breach.

Periodically, Ravi's smartphone receives mHealth software updates, because the software comes with a maintenance contract. Security-related patches are automatically installed, and new features are optionally installed. This remote manageability **(P16-manageable)** protects Ravi's PII and keeps Ravi's interest with the addition of novel features.

After one month, Ravi's smartphone is stolen while he is at the gym. With one call to his cellular carrier, his old phone is remotely disabled (destroying all the keys and PII stored on the phone) and a new phone is sent by courier. Fortunately, Ravi's service contract (with the mHealth software provider) also supports him in the case of a lost device, so the new phone arrives pre-configured with the necessary software and encryption keys, and automatically recognizes the sensors Ravi had paired with his earlier phone.

7. RESEARCH QUESTIONS

In this section, we highlight some of the key research problems that must be solved to realize an mHealth system that possesses the properties described in Section 5.

1. **Consent Management:** How can patients use their mobile node (MN) to easily manage consent, i.e., express preferences over collection, dissemination and retention of PHI, and make consent decisions when requests occur? Usable and accessible interfaces are key.

2. **MN Architecture:** How should MN hardware and software architecture change to help protect patient privacy and enable them to manage privacy? For example, what hardware and software enhancements would help enforce patient privacy preferences? In what way are these enhancements different from those required to support other functional and security properties?

3. **Enforcing control over data:** How can patient privacy policies be securely bound to personal health information (PHI) and enforced on PHI data (for example, auto-destruct data after a specified time limit, limit the number of views, limit the number of copies, or identify the entity responsible for copying data)?

4. **Data identity:** How can patient data be labeled such that consumers of that data (e.g., doctors) can verify the assertion that this data belong to this patient, without compromising patient privacy?

5. **Anonymization:** What are effective algorithms to anonymize PII before disclosing it to another party, e.g., for research or for a medical opinion?

6. **Accountability:** What mechanisms can be used to support accountability (i.e., make consumers of PHI accountable to the patient for using PHI according to her preferences) and non-repudiation?

7. **Ecosystem**: What are the ecosystem support roles in an mHealth system? We have initially identified five roles (Figure 1); policy makers, certification bodies, manufacturers, distribution & management, and a public-key infrastructure. What policy and legal frameworks need to be in place for them to serve these roles?

8. **Tradeoffs**: Solutions to the problems above involve many tradeoffs, such as between anonymity and accountability, or patient authenticity and privacy. An important research challenge, then, is to develop a conceptual working framework to help identify these tradeoffs within a solution space and choose an appropriate balance when making design decisions.

8. SUMMARY

This paper makes four primary contributions. First, we compare existing privacy frameworks, with an eye to mobile healthcare and home-care systems. We quote or paraphrase the top-level principles given in each framework, then compare and contrast the frameworks, identifying key differences and shortcomings. Second, we identify a privacy framework for such systems, using the Common Framework as a core and drawing a few principles from other frameworks. No one framework captured all of the privacy principles we believe should be followed. Third, we extract a set of privacy properties intended for use by those who design systems and applications for mobile healthcare and home-care systems, linking them back to the privacy principles. Finally, we list several important research questions that the community should address.

We hope that the privacy framework in this paper can help to guide the researchers and developers in this community, and that the privacy properties provide a concrete foundation for privacy-sensitive systems and applications for mobile healthcare and home-care systems. There remain many technical challenges to realize these properties, given the constraints of mobile systems and the need to present *usable* interfaces on tiny devices to patients and providers (many of whom have limited technology background).

In mobile healthcare and home-care systems, the potential is great, the opportunities endless, and the challenges exciting. Let's all be sure that patient privacy remains one of the core requirements.

9. REFERENCES

[1] University of Washington. Assisted Cognition project at UW. http://www.cs.washington.edu/assistcog, visited Mar. 2008.

[2] Georgia Institute of Technology. Aware Home project at GA Tech. http://www.cc.gatech.edu/fce/ahri/, visited Mar. 2008.

[3] Asia-Pacific Economic Council (APEC). APEC privacy framework, 2005. http://preview.tinyurl.com/cusnax.

[4] R. Aylward and J. A. Paradiso. A compact, high-speed, wearable sensor network for biomotion capture and interactive media. In *Proceedings of the Sixth International Conference on Information Processing in Sensor Networks (IPSN)*, pages 380–389. ACM Press, Apr. 2007. DOI 10.1145/1236360.1236408.

[5] C. R. Baker, et al. Wireless sensor networks for home health care. In *Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops*, pages 832–837. IEEE Computer Society, May 2007. DOI 10.1109/AINAW.2007.376.

[6] S. A. Buckovich, H. E. Rippen, and M. J. Rozen. Driving toward guiding principles: A goal for privacy, confidentiality, and security of health information. *Journal of the American Medical Informatics Association*, 6(2):122–133, Mar.–Apr. 1999.

[7] Certification Commission for Healthcare Information Technology (CCHIT). Consumer's guide to certification of personal health records, 2008. http://cchit.org/files/CCHITPHRConsumerGuide08.pdf.

[8] Center for Democracy & Technology. Comprehensive privacy and security: Critical for health information technology. White paper, May 2008. http://www.cdt.org/healthprivacy/20080514HPframe.pdf.

[9] Center for Democracy & Technology. Summary of health privacy provisions in the 2009 economic stimulus legislation, 29 Apr. 2009. http://www.cdt.org/healthprivacy/20090324_ARRAPrivacy.pdf.

[10] Y. B. Choi, K. E. Capitan, J. S. Krause, and M. M. Streeper. Challenges associated with privacy in

healthcare industry: Implementation of HIPAA and security rules. *Journal of Medical Systems*, 30(1):57–64, Feb. 2006. DOI 10.1007/s10916-006-7405-0.

[11] S. P. Cohn, National Committee on Vital and Health Statistics. Privacy and confidentiality in the nationwide health information network, June 2006. http://www.ncvhs.hhs.gov/060622lt.htm.

[12] Intel Research. Digital Home project at Intel. http://www.intel.com/research/exploratory/digitalhome.htm, visited Mar. 2008.

[13] D. Halperin, Thomas, K. Fu, T. Kohno, and W. H. Maisel. Security and privacy for implantable medical devices. *IEEE Pervasive Computing*, 7(1):30–39, Jan.–Mar. 2008. DOI 10.1109/MPRV.2008.16.

[14] US Department of Health and Human Services. Your health information: Privacy rights. http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/consumer_rights.pdf, visited Mar. 2009.

[15] Health Privacy Working Group, Health Privacy Project. Best principles for health privacy. Georgetown University, July 1999.

[16] Health Privacy Project. Best practices for employers offering personal health records (PHRs). Developed by the Employers' Working Group on Personal Health Records (PHRs), Dec. 2007. http://www.cdt.org/healthprivacy/2007Best_Practices.pdf.

[17] International Security, Trust, and Privacy Alliance. Privacy framework, Oct. 2002. http://www.istpa.org/pdfs/ISTPAPrivacyFrameworkV1.1.pdf.

[18] International Security, Trust, and Privacy Alliance. Analysis of privacy principles: Making privacy operational, May 2007. http://www.istpa.org/pdfs/ISTPAAnalysisofPrivacyPrinciplesV2.pdf.

[19] D. Kaplan. Group unveils first-of-its-kind standard to secure patient data. *SC Magazine*, Mar. 2009. http://preview.tinyurl.com/clvu9r.

[20] P. Kulkarni and Y. Öztürk. Requirements and design spaces of mobile medical care. *SIGMOBILE Mobile Computing Communications Review*, 11(3):12–30, July 2007. DOI 10.1145/1317425.1317427.

[21] B. O. Lubeke and V. M. Lubecke. Wireless house calls: using communications technology for health care and monitoring. *IEEE Microwave Magazine*, 3(3):43–48, Sept. 2002. DOI 10.1109/MMW.2002.1028361.

[22] D. C. Mack, M. Alwan, B. Turner, P. Suratt, and R. A. Felder. A passive and portable system for monitoring heart rate and detecting sleep apnea and arousals: Preliminary validation. In *Proceedings of the First Transdisciplinary Conference on Distributed Diagnosis and Home Healthcare (D2H2)*, pages 51–54. IEEE Computer Society, Apr. 2006. DOI 10.1109/DDHH.2006.1624795.

[23] M. Meingast, T. Roosta, and S. Sastry. Security and privacy issues with health care information technology. In *Proceedings of the 28th IEEE EMBS Annual International Conference*, Aug. 2006. DOI 10.1109/IEMBS.2006.260060.

[24] Markle Foundation. Common Framework for networked personal health information: Overview and principles. Connecting For Health, June 2008. http://connectingforhealth.org/phti/docs/Overview.pdf.

[25] Wikipedia. mHealth. http://en.wikipedia.org/wiki/Mhealth, visited Apr. 2009.

[26] National Committee on Vital and Health Statistics. Individual control of sensitive health information accessible via NHIN. NCVHS letter to HHS Secretary, Feb. 2008. http://www.ncvhs.hhs.gov/080220lt.pdf.

[27] Organization for Economoic Co-operation and Development. OECD guidelines on the protection of privacy and transborder flows of personal data. http://preview.tinyurl.com/2of8ox, visited Aug. 2009.

[28] Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services. The nationwide privacy and security framework for electronic exchange of individually identifiable health information, Dec. 2008. http://www.hhs.gov/healthit/privacy/framework.html.

[29] R. Paradiso, G. Loriga, and N. Taccini. A wearable health care system based on knitted integrated sensors. *IEEE Transactions on Information Technology in Biomedicine*, 9(3):337–344, Sept. 2005. DOI 10.1109/TITB.2005.854512.

[30] Intel Research. PlaceLab project at Intel. http://www.placelab.org/, visited Mar. 2008.

[31] C. Pounder. Why the APEC privacy framework is unlikely to protect privacy. Out-Law.com, Oct. 2007. http://www.out-law.com/default.aspx?page=8550.

[32] W. B. Rouse. Health care as a complex adaptive system: Implications for design and management. *The Bridge*, 38(1), Spring 2008.

[33] University of Rochester. Smart Home project at Center for Future Health. http://www.futurehealth.rochester.edu/smart_home, visited Mar. 2008.

[34] V. Stanford. Pervasive health care applications face tough security challenges. *IEEE Pervasive Computing*, 1(2):8–12, Apr.–June 2002. DOI 10.1109/MPRV.2002.1012332.

[35] Vital Wave Consulting. mHealth for development: The opportunity of mobile technology for healthcare in the developing world. United Nations Foundation and Vodafone Foundation Technology Partnership, Feb. 2009. http://www.unfoundation.org/global-issues/technology/mhealth-report.html.

[36] U. Varshney. Pervasive healthcare and wireless health monitoring. *Mobile Networks and Applications*, 12(2-3):113–127, June 2007. DOI 10.1007/s11036-007-0017-1.

[37] Q. Wang, W. Shin, X. Liu, Z. Zeng, C. Oh, B. K. Alshebli, M. Caccamo, C. A. Gunter, E. Gunter, J. Hou, K. Karahalios, and L. Sha. I-Living: An open system architecture for assisted living. In *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics (SMC)*, volume 5, pages 4268–4275, Oct. 2006. DOI 10.1109/ICSMC.2006.384805.