1-2011

A Threat Taxonomy for mHealth Privacy

David Kotz
Dartmouth College

A threat taxonomy for mHealth privacy

David Kotz
Institute for Security, Technology, and Society
Department of Computer Science
Dartmouth College
Hanover, NH 03755 USA

***Abstract*—Networked mobile devices have great potential to enable individuals (and their physicians) to better monitor their health and to manage medical conditions. In this paper, we examine the privacy-related threats to these so-called *mHealth* technologies. We develop a taxonomy of the privacy-related threats, and discuss some of the technologies that could support privacy-sensitive mHealth systems. We conclude with a brief summary of research challenges.**

I. Introduction

Healthcare information technology has potential to improve healthcare quality, improve efficiency, and reduce cost, and is currently on the cusp of major innovations and widespread deployment around the world. In this paper, we specifically examine the privacy challenges involved in *mobile* computing and communications technologies used for personal-health monitoring. Such **mHealth** technology 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, and reducing the cost of care by allowing patients to spend less time in the hospital or make fewer visits to their doctor. The UN Foundation recently formed the *mHealth Alliance* specifically to explore and promote the value of mobile computing technologies in improving healthcare in developing nations [1].

In mHealth, Mobile Internet Devices (MIDs), connected wirelessly to wearable, portable, and even embeddable sensors, will enable long-term continuous medical monitoring 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), 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, using the capitalized form as a reminder of its broader meaning.) The resulting data may be used directly by the Patient [2] or may be shared with a physician for treatment [3], with an insurance company for coverage, with a scientist for research [4], with a coach for athletic training [5], or with family members and friends in social-networking communities targeted towards health and wellness [6]. These citations are only examples.

A. The Challenge

Although mHealth systems may indeed improve quality of healthcare and to improve quality of life, they also generate new security and privacy issues [7]. In this paper, we focus on privacy; it is therefore 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" [8]. We also follow NCVHS and define PHI as "personal health information."

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-related* information to be collected, not just 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 medication regimen), with lifestyle coaches (e.g., diet advisers), with athletic coaches (e.g., sports teams or health-club trainers), 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. In an earlier paper [9], we present a privacy framework for mHealth, built on well-known healthcare privacy frameworks. In this paper, we contribute a taxonomy of threats for mHealth privacy, and survey some existing technical solutions to those challenges.

B. Background

In many cases, the data collected by mHealth devices will be incorporated into a medical record. There are at least two

978-1-4244-8953-4/11/$26.00

broad categories of medical records. An Electronic Health Record (EHR) is created and managed by a healthcare provider (hospitals and other clinical organizations), whereas a Personal Health Record (PHR) is created and managed by the Patient herself. Since PHRs pose at least as many privacy challenges as EHRs, we focus primarily on PHRs in this paper.

In the *patient-centric PHR* model, typified by Google Health [10] and Microsoft's HealthVault [11], Patients control all their PHI via web portals, including operations to create, import, update, read and delete records; both PHRs allow compatible devices to upload PHI directly to the Patient's record via wireless connections to the Internet. Patients are allowed to share information in their PHRs with external health service providers, caregivers, coaches, trainers and doctors.

Another common case is the *vendor-supplied PHR*, in which an mHealth-device vendor provides an application-specific record of the data collected by that device, accessible to the Patient on the vendor's website. The mHealth-related privacy issues in such a system are the same as those in the patient-centric PHRs mentioned above. We expect Patients will be challenged, however, to manage their privacy across multiple PHRs, and to understand the subtle complexities of their trust relationships with vendors, wireless carriers, Internet service providers, and healthcare providers.

Architecture and Terminology: 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, location) or physiology (electrocardiograms, pulse oximeters, blood-glucose meters, weight scales). These sensors may be carried by the Patient, worn by the Patient, embedded in their living space, or implanted in their body. The sensors communicate with the MN through a wireless 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 PHR. The MN also serves as the Patient's primary interface to the PHR, with respect to managing the data-collection process and subsequent sharing of the data.

The Consumers of these records (including doctors and other clinical personnel, insurance companies and other billing-related personnel, researchers and regulators) access the PHR through some Client computer. The security issues on this platform are largely out of scope of this paper.

In this paper we focus on the *mobile* aspects of the infrastructure, and the associated networks to support mobility. Mobility and networking bring many risks: the sensor data may be intercepted (impacting privacy), tampered with (leading to incorrect data and care decisions), or blocked (leading to loss of 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. Finally, since we expect that Patients would like to use their existing mobile phone as their MN, these risks are compounded because health-sensing tasks must share the phone with email and other activities that open the platform to compromise.

Although any viable solution, and any real deployment, will doubtless be more complex than implied by the above description, this architecture provides a structural basis and terminology for our discussion of prior work and upcoming research challenges, below.

C. Contributions

We make three broad contributions in this paper:

1) we identify a taxonomy of privacy threats in mHealth,
2) we survey prior work and existing technologies, and
3) we identify several important research challenges.

II. Threat taxonomy

Recalling the NCVHS definition of privacy (in a healthcare setting) as the user's right to "control the acquisition, uses, or disclosures of his or her identifiable health data" [8], a threat to user privacy is the possibility that his right to control his PHI is weakened or eliminated due to erroneous or malicious actions. When these threats are realized, the consequences can be severe: exposure of identifiable Patient health data leading to loss of money or reputation, time spent recovering from medical identity theft, harm to health, or even death.

Table I summarizes these threats, organized by the type of threat: mis-use of Patient identities, unauthorized access or modification of PHI, or disclosure of PHI. For each category, we consider three types of adversary: the *Patient* himself or herself, *insiders* (authorized PHR users, staff of the PHR organization, or staff of other mHealth support systems), and *outsiders* (third parties who act without authorization).

In the following subsections, we survey existing technological approaches to mitigate these and related threats. Although this survey cannot be comprehensive, due to the limited length of this paper, we draw on the literature in healthcare information technology, mobile computing, pervasive computing, wireless networks, sensor networks, cryptography, and computer security.

A. Identity threats

In the first section of Table I we explore threats related to Patient identity. There are three concerns here. First, the Patient may lose (or share) their identity credentials, enabling others to have access to their PHI in the PHR (or in their MN). Second, insiders may use Patient identities for medical fraud, for example, by submitting fraudulent insurance claims [12]; the result can be financially or even medically damaging to the Patient. Furthermore, in the growing problem of medical identity theft, outsiders (or insiders) may use a Patient's identity to obtain medical services [13], potentially with financial or medical damage to the Patient. Finally, in some settings (such as research) Patient identities are removed from the PHI, and the risk is that an outsider may combine the de-identified data with data from another source to re-identify the Patients, that is, to re-link Patient identity to their PHI [14].

The most relevant work addresses authentication, anonymization and re-identification.

TABLE I
PRIVACY-RELATED THREATS IN MHEALTH SYSTEMS

Identity threats: mis-use of patient identities	
patients	leave PHR credentials on public computer (identity loss)
patients	share passwords with outsiders (identity sharing)
patients	reveal passwords to outsiders (social-engineering attack)
insiders	mis-use identities to obtain reimbursement (insurance fraud) [12]
insiders	mis-use identities to obtain medical services (identity theft) [13]
outsiders	mis-use identities to obtain medical services (identity theft) [13]
outsiders	re-identifying PHI in de-identified data sets [14]
outsiders	observe patient identity or location from communications
Access threats: unauthorized access to PHI or PHR	
patients	consent preferences, as expressed, do not match those desired
patients	intentional (or unintentional) access beyond authorized limit
patients	mistaken modifications, because of over-privilege or inadequate controls
insiders	mistaken modifications, because of over-privilege or inadequate controls [15]
insiders	intentional unauthorized access, for curiosity or malice [15], [16]
insiders	intentional modifications, to obtain reimbursement (insurance fraud) [12]
outsiders	intentional unauthorized access, for curiosity or malice [17]
outsiders	intentional modifications, for fraud or malice [17]
Disclosure threats: unauthorized disclosure of PII and PHI	
data at rest, in the PHR:	
patients	inadvertent disclosure due to malware or file-sharing tools [13]
insiders	inadvertent disclosure due to malware or file-sharing tools [13]
insiders	inadvertent disclosure due to sharing passwords [15]
insiders	intentional disclosure, for profit or malice [16]
outsiders	intentional disclosure, for profit or malice [16]
data at rest, in the mobile devices:	
patients	loss of MN or SN exposes PHI, keys, SN types, sensing tasks
outsiders	theft of MN or SN exposes PHI, keys, SN types, sensing tasks
data in transit:	
outsiders	eavesdrop on SN-MN, MN-PHR, PHR-PHR, PHR-client; traffic analysis and/or content decryption [18, for example]
outsiders	observe presence and type of sensors on patient [19]

1) Authentication: Authentication protocols and mechanisms are used to authenticate the Patient (to ensure that the correct Patient is being sensed), to authenticate the provider (to ensure that only authorized personnel have access to the medical equipment or sensor data), and to authenticate devices (to ensure that only valid sensing equipment can participate, and that data is sent to the authentic information systems).

Authenticating the Patient. The most common method of authenticating Patients to a PHR or other healthcare IT system is to verify a combination of their username and password. Of course, this method is susceptible to a variety of well-known attacks. Some PHR providers are testing or deploying two-factor authentication [20].

In mHealth applications there are additional challenges. The data consumers need to be sure that the data collected by sensors is collected from the correct Patient; otherwise the data may be interpreted incorrectly and result in treatment errors or incorrect conclusions in research or public-health monitoring [21]. It may be possible to use biometric data for authentication, or more correctly, for identity verification [22, for example]. Several research studies propose methods based on features from electrocardiography (or similar biometrics) to verify Patient identity [23]. It remains an open problem to find a robust biometric that is usable, inexpensive, and reliable under a range of Patient activities.

Authenticating the provider. HIPAA states that covered entities must "implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed" [24], and the 2009 HITECH Act extends this rule to business associates [25]. Most of the issues here are the same as for authenticating Patient access, above. The US Department of Veterans affairs has implemented "single sign-on" authentication to enable users to easily access multiple portals of the department using only one set of government issued credentials.

The National Health Service (NHS), in the UK, is one of the largest national-scale EHR projects underway anywhere. The NHS Care Records Service (CRS) is a secure service that links patient information from different parts of the NHS, enabling authorized NHS staff and patients to have access to health information [26]. A registration authority within each healthcare organization is responsible for verifying the identities of healthcare professionals and support staff, and to register all caregivers allowed to access CRS. The registration authority issues a smart card to each caregiver; the smart card is printed with the user's name, photo and a unique identity number. The system uses these cards and identities to provide role-based access to patient information. However, there have been reports of "inappropriate access" by sharing of passwords and PINs by the staff, which poses a serious insider risk [27].

Authenticating devices. Consider our reference architecture. When a mobile node (MN) communicates with sensor nodes (SNs), it must determine whether they are *authentic* sensors, that is, they are *valid* (truly the sensors they claim to be), *untampered* (not compromised by an adversary), and *correct* (they are the specific instances attached to the desired Patient, not another Patient nearby). Similarly, the SNs must determine whether the MN requesting data is the correct MN, that is, the one authorized to receive sensor data. Finally, MNs provide reports to, or obtain configuration from, healthcare services; these transactions also require mutual authentication so that the service believes the data comes from the correct MN (really, the correct Patient), and the MN believes the data is sent to (or configuration comes from) an authorized healthcare service.

Fundamentally, these authentication challenges may be easily solved by asymmetric cryptography and a public-key infrastructure. The problem is not so simple, however, for five reasons. First, these mobile devices are necessarily small and their resources are limited; asymmetric cryptography is computationally expensive. Second, these devices are often disconnected from the Internet, or have a weak connection to the Internet, obviating solutions that assume a live connection to (for example) a certificate authority. Third, these devices are small and may be easily lost or stolen, leading to a loss or exposure of embedded keys. Fourth, key distribution and key storage require secure and *easy-to-use* solutions, and yet some nodes have little or no human interface. Finally, some of the devices (notably the MN) may be owned and configured by the Patient rather than by the medical device manufacturer or

healthcare provider.

We have seen few solutions in the literature that attempt to address the broad key-management challenge in the context of mHealth. One approach considers mote-class sensor nodes and demonstrates techniques for secure key exchange, biometric methods to authenticate the Patient, and an encryption protocol to protect the sensor data [28]. Others have demonstrated that it is feasible and inexpensive to couple mote-class sensor nodes with hardware-encryption support like that in a TPM [29].

Finally, since mobile devices like the MN and SN can be easily lost or stolen, secure key storage is an important challenge lest the keys become available to an adversary.

2) Anonymity: The HIPAA Privacy Rule states that covered entities may use or disclose PHI that is de-identified without restriction [30]. Covered entities that seek to release such PHI must determine that the information has been de-identified using either statistical methods to verify de-identification or by removing certain parts of the PHI as specified in the Rule. Under the Rule, a covered entity can de-identify PHI by removing all 18 elements that could be used to identify the Patient or the Patient's relatives, employers, or household members. The Rule also requires the covered entity to have no actual knowledge that the remaining information could be used alone or in combination with other information to identify the Patient. The HITECH Privacy Rule does not add anything new to this section of the HIPAA Privacy Rule.

B. Access threats

In the next section of Table I we explore threats related to unauthorized access to PHI, whether in the MN or the PHR. The first threat comes from the Patient himself or herself, because (under the definition of health information privacy) the Patient has a right to control the collection, use, and disclosure of PHI; if the Patient fails to express their consent consistent with their actual preference, for whatever reason, they may allow broader-than-intended collection, access or disclosure.

Insiders may "peek" at Patient data, out of curiosity, or with the intent to harm the Patient (e.g., an employer who snoops on employer-provided PHR and fires workers with expensive conditions) [15], [16]. Outsiders may break into Patient records, which may lead to embarrassment (e.g., exposing a Patient's psychiatric data to his divorced spouse) [17].

Several of these threats involve the modification of health records. In a PHR, Patients (or insiders [15]) may mistakenly modify their data if the access-control policies are too permissive, or if the mechanisms too easily allow mistakes. Insiders may modify PHI intentionally, to obtain reimbursement via insurance fraud [12]. Outsiders may also modify a Patient's PHI, for fraud or malice [17].

In this subsection we survey work on consent management (allowing the Patient to determine what access is permitted), access control (policies and mechanisms), auditing (to support detection of violations), and data integrity.

1) Consent Management: A common legal requirement is that PHR service or healthcare providers obtain consent from a Patient before disseminating her medical records to other providers or to entities such as a marketing department, medical researchers, or public-health officials. Presenting the privacy policy in an understandable format – such that the Patient can set her preferences to provide or withhold consent – is a major challenge. Bellman et al. describe risks to Patient privacy due to the manner in which "opt-in" or "opt-out" questions are posed on a consent form [31]. The Healthcare IT Standards Panel (HITSP), a public-private partnership between US governments (federal and state) and health-related organizations, has released an interoperability standard specifying the management of machine-interpretable "consent directives" that Patients may issue to healthcare organizations on the access, collection, use and disclosure of their data [32].

2) Access Control: A mechanism for controlled access to a Patient's PHI, which restricts access to only legitimate entities, is necessary to ensure Patient privacy. Standards bodies in the US, such as HL7 Standards Development Organization, have chosen the Role Based Access Control (RBAC) model [33] to enforce access control in traditional healthcare IT systems. Although RBAC is not "privacy-aware" (access is either granted or denied), Ni et al. discuss how to extend standard RBAC to make it "privacy-aware" and enforce authorizations at a finer level of granularity [34]. The RBAC model fits well in an organized healthcare setting, such as a hospital, because each entity in a hospital has a specific role and follows a well-defined hierarchy. On the other hand, identifying roles and managing role membership is difficult in large organizations. And, certain features, such as "break-the-glass" to override access control rules in medical emergencies, do not exist in traditional RBAC [35].

3) Auditing: Both HIPAA [24] and HITECH [25] require users within the healthcare provider's organization to be held accountable for their actions when handling Patients' protected health information. There are different approaches to maintaining audit controls for such information; one approach [36] specifies a profile for the Audit Trail that contains sufficient information to answer questions such as: "For some user: which Patient's PHI was accessed? For some Patient PHI: which users accessed it? What user authentication failures were reported?" Such approaches help detect unauthorized access, illegal disclosure of PHI, and attempts by hackers to break into a PHR system.

4) Data integrity: HIPAA [24] states that covered entities must "implement policies and procedures to protect electronic PHI from improper alteration or destruction". In an mHealth setting, the Patient's MN is responsible for confidentiality and integrity of the data, at least within the body-area network; typical solutions include encryption or a cryptographically-secure hash. Again, because key management is fundamental to achieving data confidentiality, there is a need to investigate mechanisms for key management in mobile environments.

C. Disclosure threats

In the final section of Table I we explore threats related to the disclosure of PHI, including data at rest and data in transit.

We now survey work related to secure data transmission, device presence, and device compromise and theft.

1) Secure Transmission: Although both HIPAA [24] and HITECH [25] require secure communication between HIPAA-covered entities, our concern here is an adversary who wishes to obtain confidential medical information from observing the network communications between the MN and its SNs, or between the MN and the distant health services. In the mHealth setting, we must assume the use of wireless networks and open standards. There are four fundamental challenges.

First, the adversary may inspect the wireless-network packets and obtain sensitive medical data; this problem can be resolved by encrypting all communications with a secure encryption method and an appropriately strong encryption key. Most emerging services use HTTP over SSL, but we know of one approach leveraging SIM-card support in mobile phones [37]. Key management remains a challenge, however.

Second, even if the wireless-network traffic is encrypted, in some settings it is possible for a clever adversary to use traffic analysis to determine characteristics of the traffic [38]. It may be possible, for example, to determine the type of sensor node from the pattern of its communications, or the type of medical application by observing the pattern of MN communications [18].

Third, the adversary may use physical-layer or link-layer fingerprinting methods to identify the device type. In general, fingerprinting techniques observe subtle differences in the network behavior of devices, because of implementation differences across manufacturers, models, revisions, or even individual devices [39, for example].

Fourth, because the wireless medium is open, an active adversary may inject frames or may selectively interfere with (cause collisions with) wireless frames. These methods may enable the adversary to create a man-in-the-middle situation, to use link-layer fingerprinting methods, or to compromise the devices in a way that divulges their secrets. Indeed, there are increasing concerns (and demonstrated attacks) regarding the wireless communications of implanted medical devices [19].

2) Device presence: A Patient may consider the fact that they are using personal medical sensors to be private information; a Patient may not want an employer to know, for example, that she is wearing a fetal monitor. The challenge, then, is to allow MN-SN communication, without exposing to an eavesdropper the fact that they are *medical* devices, nor to allow the adversary to track the Patient's location via recognizable device identifiers. We are unaware of any research specific to the mHealth context. Most of the relevant work relates to network-identifier privacy [40, for example, about Wi-Fi]. It remains to be seen whether there is a standards-compliant solution in which the link-layer identifiers (and other fields related to link-layer discovery) can be constructed to not leak information about sensor type.

3) Device compromise, theft: The Patient's MN may be compromised, for example, by an email-borne virus. The MN or SN devices may be lost or stolen. In any case there are several risks. The adversary may obtain access to personal health information, or learn the type of sensor nodes, both of which may expose information about the Patient's medical condition. Moreover, any key material may be obtained by the adversary, potentially allowing the adversary to decrypt previous, current, or future communications between the Patient's MN and SNs, or between the MN and the PHR. Furthermore, the key material may enable the adversary to inject false data into the MN or health records system, or even to reconfigure the Patient's other devices. Finally, the key material may enable the adversary to decrypt data stored in the PHR. The specific risks depend on the protocols used for data transfer, on the encryption methods used, and on the security of key generation, distribution, revocation, and storage. We have not seen any complete solution to this problem in the literature.

A possibly more insidious threat is the unintended disclosure of sensor data by applications installed by the user, including applications unrelated to healthcare. The security community is just beginning to address this threat [41].

III. Summary and research questions

We believe it is essential to consider privacy in the design and implementation of any mHealth system, given the sensitivity of the data collected. In this paper we outline a threat taxonomy for mHealth privacy, and we discuss some the technologies that could support privacy-sensitive mHealth systems. Because of page limitations, our survey is necessarily not comprehensive.

Much research remains; consider, for example, the following questions. How can the Patient use their MN to easily manage consent, i.e., express preferences over collection, dissemination and retention of PHI, and make consent decisions when requests occur? How should MN hardware and software architecture change to help protect Patient privacy and enable them to manage privacy? What technology would help to *enforce* control over PHI? What solutions provide reliable Patient identity verification and preserve Patient privacy in the process? What are effective algorithms to anonymize PII before disclosing it to another party, e.g., for research or for a medical opinion? What mechanisms can be used to support accountability and non-repudiation? What support services does an mHealth system need? Consider policymakers, certification bodies, manufacturers, remote management, and a key-management infrastructure. Finally, how does one address the inevitable trade-offs (e.g., between anonymity and accountability, or Patient authenticity and privacy)?

Acknowledgements

This research results from a program at the Institute for Security, Technology, and Society at Dartmouth College, supported by Intel Corporation, by NSF Trustworthy Computing award 0910842, and by the Department of Health and Human Services (SHARP program) under award number 90TR0003-01. Many thanks to colleagues at Intel and Dartmouth for their feedback, particularly Amit Baxi and Sasikanth Avancha.

REFERENCES

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

[2] 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 *Proc. IEEE International Conference on Systems, Man and Cybernetics (SMC)*, vol. 5. IEEE Press, Oct. 2006, pp. 4268–4275. DOI 10.1109/ICSMC.2006.384805

[3] (2008, Mar.) Smart Home project; Center for Future Health, Univ. Rochester. Online at http://www.futurehealth.rochester.edu/smart_home

[4] (2008, Mar.) Digital Home project at Intel. Intel Research. Available online: http://www.intel.com/research/exploratory/digitalhome.htm

[5] R. Aylward and J. A. Paradiso, "A compact, high-speed, wearable sensor network for biomotion capture and interactive media," in *Proc. International Workshop on Information Processing in Sensor Networks (IPSN)*. ACM Press, Apr. 2007, pp. 380–389. DOI 10.1145/1236360.1236408

[6] (2009, Oct.) Dailystrength.org. Daily Strength. Available at http://www.dailystrength.org/

[7] M. Meingast, T. Roosta, and S. Sastry, "Security and privacy issues with health care information technology," in *Proc. IEEE Engineering in Medicine and Biology Society Conference (EMBS)*. IEEE Press, Aug. 2006. DOI 10.1109/IEMBS.2006.260060

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

[9] D. Kotz, S. Avancha, and A. Baxi, "A privacy framework for mobile health and home-care systems," in *Proc. Workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS)*. ACM Press, Nov. 2009, pp. 1–12. DOI 10.1145/1655084.1655086

[10] (2008, Nov.) Google Health. Available at https://www.google.com/health

[11] (2008, Nov.) Microsoft HealthVault– web-based PHR. Microsoft. Available at http://www.healthvault.com

[12] P. Dixon, "Medical identity theft: The information crime that can kill you," The World Privacy Forum, May 2006. Available at http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf

[13] M. E. Johnson, "Data hemorrhages in the health-care sector," in *Financial Cryptography and Data Security*. Springer-Verlag, Feb. 2009. DOI 10.1007/978-3-642-03549-4_5

[14] B. Malin, "Re-identification of familial database records," in *AMIA Annual Symposium Proc.*. AMIA, Nov. 2006, pp. 524–528. Available at http://view.ncbi.nlm.nih.gov/pubmed/17238396

[15] S. Sinclair and S. W. Smith, "Preventative directions for insider threat mitigation via access control," in *Insider Attack and Cyber Security: Beyond the Hacker*. Springer-Verlag, 2008, vol. 39, pp. 173–202. DOI 10.1007/978-0-387-77322-3_10

[16] A. Appari and M. E. Johnson, "Information security and privacy in healthcare: Current state of research," Proc. Workshop on Information Security and Privacy (WISP), Aug. 2008. Available at http://www.ists.dartmouth.edu/library/416.pdf

[17] E. Messmer, "Health care organizations see cyberattacks as growing threat," *Network World*, Feb. 2008. Available at http://tinyurl.com/66b2py

[18] V. Srinivasan, J. Stankovic, and K. Whitehouse, "Protecting your daily in-home activity information from a wireless snooping attack," in *Proc. of Ubiquitous Computing (UbiComp)*. ACM Press, Sep. 2008, pp. 202–211. DOI 10.1145/1409635.1409663

[19] D. Halperin, Thomas, K. Fu, T. Kohno, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 30–39, Jan.–Mar. 2008. DOI 10.1109/MPRV.2008.16

[20] J. Moore, "The feds and PHR privacy," *Government Health IT*, Jan. 2009. Available at http://www.govhealthit.com/Articles/2009/01/26/The-feds-and-PHR-privacy.aspx

[21] C. Cornelius and D. Kotz, "On usable authentication for wireless body area networks," in *USENIX Workshop on Health Security (HealthSec)*, August 2010, position paper. Available at http://www.cs.dartmouth.edu/~dfk/papers/cornelius-healthsec10.pdf

[22] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Proc. International Conference on Parallel Processing Workshops*. IEEE Computer Society, Oct. 2003, pp. 432–439. DOI 10.1109/ICPPW.2003.1240399

[23] J. Sriram, M. Shin, T. Choudhury, and D. Kotz, "Activity-aware ECG-based patient authentication for remote health monitoring," in *Proc. Intl. Conf. on Multimodal Interfaces and Workshop on Machine Learning for Multi-modal Interaction (ICMI-MLMI)*, Nov. 2009.

[24] M. Scholl, K. Stine, J. Hash, P. Bowen, A. Johnson, C. D. Smith, and D. I. Steinberg, "An introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) security rule," National Institute of Standards and Technology, Tech. Rep. 800-66-Rev1, Oct. 2008. Available at http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

[25] (2009, Nov.) HITECH Act expands HIPAA privacy and security rules. Coppersmith Gordon Schermer and Brockelman. Available at http://www.azhha.org/member_and_media_resources/documents/HITECHAct.pdf

[26] (2009, Mar.) Connecting for Health: Systems and Services. UK National Health Service. Available at http://www.connectingforhealth.nhs.uk/systemsandservices

[27] T. Collins, "NHS trust uncovers password sharing risk to patient data," *Computer Weekly*, Jul. 2006. Available at http://www.computerweekly.com/Articles/2006/07/11/216882/nhs-trust-uncovers-password-sharing-risk-to-patient.htm

[28] K. Malasri and L. Wang, "Design and implementation of a secure wireless mote-based medical sensor network," in *Proc. Ubiquitous Computing (UbiComp)*. ACM Press, Sep. 2008, pp. 172–181. DOI 10.1145/1409635.1409660

[29] W. Hu, P. Corke, W. C. Shih, and L. Overs, "secFleck: A public key technology platform for wireless sensor networks," in *Proc. European Conference on Wireless Sensor Networks (EWSN)*. Springer-Verlag, Feb. 2009, pp. 296–311. DOI 10.1007/978-3-642-00224-3_19

[30] (2009, Mar.) HIPAA website. Available at http://www.hipaa.org/

[31] S. Bellman, E. J. Johnson, and G. L. Lohse, "To opt-in or opt-out? it depends on the question," *Communications of the ACM*, vol. 44, no. 2, pp. 25–27, Feb. 2001. DOI 10.1145/359205.359241

[32] "TP-30: HITSP manage consent directives transaction package," Healthcare Information Technology Standards Panel, Aug. 2008. Available at http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=2&PrefixNumeric=30

[33] D. Ferraiolo and R. Kuhn, "Role based access control," in *Proc. National Computer Security Conference*. NIST, 1992. Available at http://csrc.nist.gov/rbac/ferraiolo-kuhn-92.pdf

[34] Q. Ni, D. Lin, E. Bertino, and J. Lobo, "Conditional privacy-aware role based access control," in *Proc. European Symposium On Research In Computer Security (ESORICS)*, ser. Lecture Notes in Computer Science, vol. 4734. Springer-Verlag, Sep. 2007, pp. 72–89. DOI 10.1007/978-3-540-74835-9_6

[35] G. H. M. B. Motta and S. S. Furuie, "A contextual role-based access control authorization model for electronic patient record," *IEEE Transactions on Information Technology in Biomedicine*, vol. 7, no. 3, pp. 202–207, Sep. 2003. DOI 10.1109/TITB.2003.816562

[36] (2009, Nov.) IHE profiles. IHE International. Available at http://www.ihe.net/profiles/index.cfm

[37] D. Weerasinghe, K. Elmufti, M. Rajarajan, and V. Rakocevic, "Securing electronic health records with novel mobile encryption schemes," *International Journal of Electronic Healthcare*, vol. 3, no. 4, pp. 395–416, 2007. DOI 10.1504/IJEH.2007.015320

[38] C. V. Wright, F. Monrose, and G. M. Masson, "On inferring application protocol behaviors in encrypted network traffic," *Journal of Machine Learning Research*, vol. 7, pp. 2745–2769, Dec. 2006. Available at http://portal.acm.org/citation.cfm?id=1248547.1248647

[39] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. ACM International Conference on Mobile Computing and Networking (MobiCom)*. ACM Press, Sep. 2008, pp. 116–127. DOI 10.1145/1409944.1409959

[40] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall, "802.11 user fingerprinting," in *Proc. ACM International Conference on Mobile Computing and Networking (MobiCom)*. ACM Press, Sep. 2007, pp. 99–110. DOI 10.1145/1287853.1287866

[41] W. Enck, M. Ongtang, and P. McDaniel, "On lightweight mobile phone application certification," in *Proc. ACM Conference on Computer and Communications Security (CCS)*. ACM Press, 2009, pp. 235–245. DOI 10.1145/1653662.1653691