11-10-2009

MPCS: Mobile-based Patient Compliance System for Chronic Illness Care

Guanling Chen
University of Massachusetts Lowell

Bo Yan
University of Massachusetts Lowell

Minho Shin
Dartmouth College

David Kotz
Dartmouth College

Ethan Burke
Dartmouth College

MPCS: Mobile-Phone Based Patient Compliance System for Chronic Illness Care

Guanling Chen,* Bo Yan,* Minho Shin,† David Kotz,† Ethan Berke‡

* Department of Computer Science, University of Massachusetts Lowell

† Institute for Security, Technology, and Society, Dartmouth College

‡ Department of Community and Family Medicine, Dartmouth Medical School,
The Dartmouth Institute for Health Policy and Clinical Practice, Dartmouth College

Abstract—More than 100 million Americans are currently living with at least one chronic health condition and expenditures on chronic diseases account for more than 75 percent of the $2.3 trillion cost of our healthcare system. To improve chronic illness care, patients must be empowered and engaged in health self-management. However, only half of all patients with chronic illness comply with treatment regimen. The self-regulation model, while seemingly valuable, needs practical tools to help patients adopt this self-centered approach for long-term care.

In this position paper, we propose Mobile-phone based Patient Compliance System (MPCS) that can reduce the time-consuming and error-prone processes of existing self-regulation practice to facilitate self-reporting, non-compliance detection, and compliance reminders. The novelty of this work is to apply social-behavior theories to engineer the MPCS to positively influence patients' compliance behaviors, including mobile-delivered contextual reminders based on association theory; mobile-triggered questionnaires based on self-perception theory; and mobile-enabled social interactions based on social-construction theory. We discuss the architecture and the research challenges to realize the proposed MPCS.

I. INTRODUCTION

There are more than 100 million Americans who are currently living with at least one chronic health condition. For example, diabetes affects 21 million and hypertension affects 74 million Americans, respectively. Expenditures on chronic diseases account for more than 75 percent of the $2.3 trillion cost of our healthcare system.[1]

Unlike acute illnesses that may be amenable to short-term intervention, chronic diseases require long-term monitoring and management, lifestyle changes, and adherence to medication regimen. It is estimated, however, that only 50% of patients suffering from chronic diseases in developed countries follow treatment recommendations [53]. Poor adherence to long-term therapies severely compromises the effectiveness of treatment, making this a critical issue in population health both from the perspective of quality of life and of health economics.

Many types of chronic illness, such as diabetes, are essentially self-managed diseases and therefore require a collaborative care model in which patients are motivated to perform optimal self-management [51]. In particular, self-monitoring is important for heightened awareness and progress tracking [11], as the foundation of the self-regulation approach for patients

[1] http://www.westwirelesshealth.org

to cope with lifestyle changes [27]. A fundamental challenge, however, is to lower the barriers and increase the motivation for patients to adopt the self-regulation approach for long-term care.

Recently, there is increasing interest in using mobile phones and wearable sensors for remote health monitoring [39], [17], [23]. On the other hand, using mobile technology to improve patient compliance is still an emerging research area. For example, Kim and Jeong have used a self-reporting system for patients to input their blood glucose level, diet and exercise diary using mobile phones; based on this information, clinicians sent optimal intervention recommendations to patients using the Short Message Service (SMS) [25]. Logan et al. proposed a mobile phone-based remote patient monitoring system for management of hypertension in diabetic patients, who are requested to report hypertension measurements twice a day and will receive compliance reminders on their phones if measurements are not received on schedule [31]. These studies have primarily focused on self-reporting, fixed-schedule reminders, and minimal non-compliance detection. Other issues that hinder the adoption of self-regulation, however, have not been addressed and whether these mobile-based tools can indeed change patients' compliance behaviors remains unclear.

In this position paper, we propose a Mobile-phone based Patient Compliance System (MPCS) for better chronic illness care. We describe the self-regulation approach used for patient-centered chronic illness care and how MPCS can address some of its limitations to facilitate its adoption in practice (Section II). The novelty of this work lies in our use of three social-behavioral theories to provide the foundational principles for the MPCS designed to positively influence patient's compliance behaviors (Section III). We outline the system architecture and describe the research challenges and opportunities in this emerging area (Section IV).

II. SELF-REGULATION MODEL

Among several frameworks for examining adaptation to chronic illness, such as biomedical or stress-coping models, the self-regulation model is considered to be most comprehensive and flexible [27]. As shown in Figure 1, a self-regulation model of patient compliance typically uses a negative feedback loop. The patient's regimen-relevant behavior is monitored and
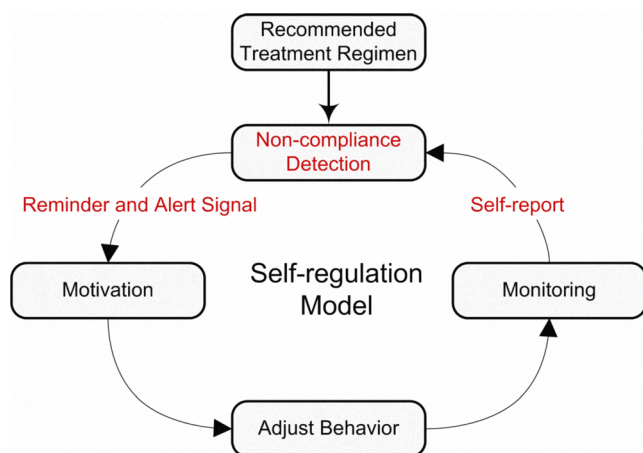
Fig. 1. The self-regulation model.

compared with the recommended treatment regimen. When deviation is detected, an error signal is generated as a feedback to the patient. If the patient is motivated to comply, he will adjust his behaviors, which will be continuously monitored for the full self-regulation loop.

In practice, patients can use a logbook for self-recording and compliance deviation can be identified during periodic patient visits. Patients themselves may be aware of non-compliance if the treatment regimen is simple enough, but it is challenging even for the motivated patients to understand the significance of occasional non-compliance. Thus the self-regulation loop can be time consuming, the raw data generated is hard to analyze, and there are few sustainable tools to keep patients aware and motivated. Next we identify several limitations of the self-regulation practice that could be improved by MPCS.

First, patients need better tools to facilitate self-reporting than traditional logbooks and periodic interviews [33]. Mobile phones, for example, are personal devices that are easily accessible to many patients. Recent phone technology includes bigger screens, faster processors, and open platforms, all of which make mobiles a good alternative for patients to record regimen-relevant activities such as medication, diet, and exercise. Furthermore, emerging medical and health-related sensors (many of which are portable and wireless) can measure patients' glucose level, blood pressure, heart rate, or activities and automatically transfer the measurements to the mobile phone, from which the data is relayed to an Internet server for storage and analysis [31]. The integrated wireless sensors and mobile phones can eliminate some of the manual-input effort to further reduce the barriers to self-reporting. The auto-sensed data is also likely to be more accurate and can better assist a clinician to detect non-compliance, to monitor symptom development and treatment progress, and to choose evidence-based intervention strategies. In addition, mobile phones can be used to automatically deliver reminders on certain actions that patients should take, such as medication and exercise [31], according to the recommended treatment regimen.

Second, it is important to know the cause(s) of patient non-

compliance for a clinician to choose an appropriate intervention strategy, since patient-tailored interventions are required for them to be effective [53]. There are many potential hard-to-predict causes of non-compliance, which could be either general or personal, such as forgetfulness, perceived lack of effect, not understanding the purpose of or the instructions for the treatment, physical difficulties, or even unattractive formulation. While the clinical team can seek this information during patient visits, the patient's answers may not be accurate (e.g., due to forgetfulness or embarrassment) and better intervention strategies may not be adopted due to the delay. Here mobile phone will be useful to deliver questionnaires seeking non-compliance cause(s) when poor compliance is detected, by comparing the recommended treatment regimen and the self-reported compliance activities. We conjecture that this feedback system will collect fine-grained non-compliance behavioral data, which when analyzed will provide the clinicians more accurate and personalized understanding of non-compliance cause(s).

Finally, patients themselves must take actions to adjust their behaviors to comply with the treatment regimen. If they are not motivated, the compliance is unlikely to improve even if non-compliance is detected and they receive pill reminders, deviation alerts, and new treatment interventions. Without motivation and commitment, the self-regulation loop is not complete and its effectiveness is questionable. Studies have shown that increasing self-awareness of their own health conditions and treatment progress has positive impact on patient compliance, and social support from patients' community is also important in influencing health outcomes and behaviors [53]. Thus mobile phones can be used as the social interaction devices that enable tighter communications with (and heightened awareness of) the patient's community, and sustain and promote patients' motivations of compliance through social influence from their community.

In summary, we propose to use MPCS to address several limitations of the self-regulation model so it can be more effectively adopted to increase patient compliance. While there are several technical challenges to realize this vision, we believe that a fundamental challenge is to engineer the system to promote "good" patient-compliance behaviors. Next we describe three social-behavior theories that guide the design of the proposed MPCS.

III. SOCIAL-BEHAVIOR THEORIES

In this section we consider several social-behavior theories that guide the system design to positively influence compliance behaviors, including mobile-delivered contextual reminders based on association theory; mobile-triggered questionnaires based on self-perception theory; and a mobile-enabled social interaction based on social-construction theory.

A. Associative Theory

A treatment regimen could potentially be too complex to remember and follow, particularly for seniors who may have multiple chronic diseases, complex treatment regimen,

or difficulties with memory. While mobile-delivered reminder systems have shown promise in improving medication compliance [31], these reminders are mostly delivered using a static schedule, such as sending a pill reminder at 8am every morning. If a pill reminder, however, is delivered out of context, such as when the patient is outside of his home, the reminder is unlikely to be useful. The question is then under what situation a reminder should be sent so patients are more likely to take actions.

The Rescorla-Wagner model, one of the principal associative theories in the area of cognitive psychology, has been used to infer human behavior for several decades [42]. According to Rescorla-Wagner model, associative mechanisms do not simply count event co-occurrences but rather evaluate those co-occurrences in a broader context of the stream of events. Namely, the context of event occurrence plays a major role of causality between events. Recently, this theory has been applied to develop a personalized reminder system for a shopping application [26].

To apply associative theory in the patient compliance domain, the context of previous compliance behaviors is important to determine the delivery of the reminders (stimulus) for better compliance (actions). For example, the analysis of a patient's self-reports may reveal that he often takes medication after completing his morning walk and returns to the kitchen. Delivering a reminder in a similar context, in theory (Rescorla-Wagner model), will more likely result in the patient's compliance in taking medicine (because of the strong association between the context and the action).

Technically, the user context (such as time, location, and activities) can be inferred using modern "smart phones," which are often equipped with a GPS sensor and accelerometer (such as the Apple iPhone and some Google Android phones) [34]. The context can be continuously monitored and recorded along with the patient's self-reports, and the data can be analyzed to model the mathematical associations between the context and the reported compliance behaviors. Next, when the user is in a similar context but has not yet made a self-report, a reminder will be delivered to his phone. We expect that this approach will work for compliance requirements with different timing constraints, and outperform the static-reminder method in improving patient compliance.

B. Self-Perception Theory

Knowing the cause(s) of poor compliance is important for the clinician to choose an intervention strategy, but it is difficult to obtain this information in traditional practice. Patients may be asked to provide an explanation during visits and interviews, but the information may not be accurate due to the patients' embarrassment or forgetfulness, or if there is a long delay between the non-compliance behaviors and the interview. The MPCS, on the other hand, can provide timely self-reports and automated non-compliance detection. Thus it is possible to automatically trigger a questionnaire on the patient's phone to ask why the treatment regimen is not followed. This tool can provide fine-grained and timely feedback to the clinician who can then choose necessary interventions.

On the other hand, there is no guarantee that the patient is willing to provide such feedback. If the patient is being asked persistently, he may even lie about the actual cause(s) of non-compliance. To improve the response rate and accuracy, we examine self-perception theory, which was developed to improve survey response rates [13]. The theory states that, based on previous studies, a survey needs to be designed and conducted in such a way that by responding to the survey, the user reduces cognitive dissonance and perceives himself as a generous and helping person. Accordingly, the triggered cause-finding questionnaire must not make patients feel that they are being blamed. Instead of explicitly asking patients about why the regimen is not followed, we suggest that the questionnaire asks patients to rate different aspects of the regimen, such as the instruction complexity, taste and smell, perceived effect, perceived side effect, difficulty to open container or to swallow a pill, cost of drugs, and so on. By using a rating system, similar to the book ratings on Amazon, patients may consider themselves to be helping the clinician improve the regimen and thus to indirectly help other patients using the similar regimen. We expect that the positive self-perception will encourage better responses to the questionnaires.

Technically, the proposed system will infer the likely cause(s) of patient's non-compliance based on his numeric ratings of a set of factors regarding his treatment regimen. It is also possible to aggregate all ratings across all the patients using the similar regimen, providing population-level statistics on non-compliance causes. The list of specific non-compliance cause(s), however, could be quite large and it may be difficult for a patient to go through multiple screens to rate every feature. Instead, we can organize the flat list into a hierarchical structure so patients can quickly navigate and select the matching option. For example, only when a patient gives a low rating (low means disagree and high means agree) on "easy to physically handle medicine," related options will then be shown, such as "easy to open bottle," "the tablets are too small to handle," or "the rectangular tablets are hard to swallow." In addition, patients should also be allowed to add a free-style comment in case some factors concerning him are not covered by the questionnaire. To minimize typing on a small screen, the mobile interface should allow patients to record an audio clip that can be analyzed by the clinician or coded by researchers.

C. Social Construction Theory

Adopting a self-regulation approach for long-term chronic illness care imposes a great life-style challenge for patients, particularly for regimen compliance when acute symptoms are not evident. The question is how to positively influence the patient and keep him motivated to comply in a continuous way. The importance of family member involvement and community support has been well recognized [53], and there are existing efforts to build websites that share patients' health data with trusted family members, and that allow a

patient community to ask and answer questions about their diseases. Studies have shown that such efforts increased patient knowledge, but were not necessarily successful in changing compliance behaviors [51]. The influence from groups that a patient encounters, including the clinical team, family members, and patient community with similar diseases, can be quite different. It remains a research challenge to understand each group's influence so we can deliberately tailor the group interactions to increase the positive influence on patient compliance.

The proposed MPCS connects patients with their community using social-construction theory, which suggests that a person will conform to others' behavior, such as adopting new technology, as consensus expectations of a workgroup in which members share similar goals [15]. In addition, if that person feels attraction to the group, the conformation will become *internalization* and lead to strong self-motivation for group compliance. Further study has also shown that social construction from a user's ego network, which is a group of friends defined by the user, also asserts strong influence on her adoption of mobile phones [8]. While social-construction theory has primarily been used for studying the influence of social factors in adoption of new technology, we believe that it will also be useful to study group influence over patients to improve compliance.

Existing efforts have mostly focused on connecting community members for question asking and answering (such as www.imedix.com). Studies have shown that such efforts increased patient knowledge, but were not necessarily successful in changing behaviors [51]. Instead, our approach leverages social-construction theory by using mobile phones to enable patients to share their regimen-relevant activities with each other, to the degree allowed by their privacy settings. Namely, a patient may browse aggregated statistics of his peer group members on the phone, such as overall daily activities (medication, diet, and exercise), average vital and health measurements and readings, and so on. The mobile-enabled social interactions allow patients to form a group sharing the same health-improvement goal for a particular chronic illness. By combining this feature with other social application features, such as status updates, community interactions, and knowledge sharing, patients are likely to be attracted to the group, as evidenced by the popularity of other social-networking sites. According to the social-construction theory, the increased attraction to the group will influence individuals to conform to group compliance behaviors, which are visible to the patients through group-level shared regimen-relevant activities and measurements.

In addition, a patient may explicitly define some group members as his buddies, such as those he knows in real life, or those introduced by the same clinician, or those he interacts with in the community but decides to establish a closer connection. A patient can receive detailed activity updates from his ego network (friends) as permitted. By observing the good compliance behaviors and treatment progress of his ego network, and "how" others have managed to follow the
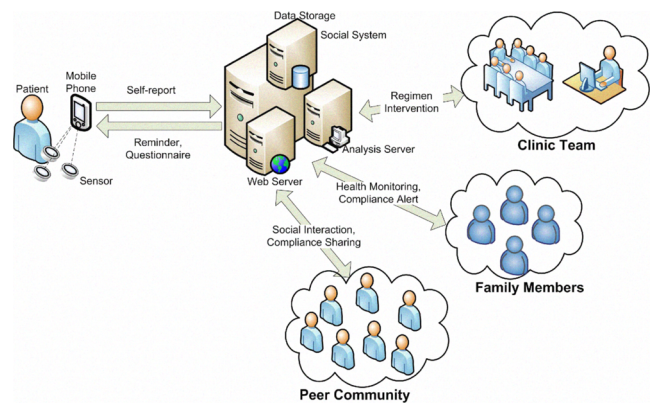

Fig. 2. The MPCS system architecture.

regimen, a patient may feel more confident and can seek skills from his buddies for better adherence.

Technically, our proposed solution will implement both a mobile client and a backend server for the social interaction system. Enough communication, support, and knowledge-sharing features must be provided to keep patients engaged. It must present community-wide statistics to increase each patient's awareness of his or her own compliance actions as they relate to the group behaviors. On the other hand, we must address privacy issues so patients can feel comfortable sharing some sensitive information (we discuss privacy below).

IV. System Architecture and Challenges

Figure 2 shows the overall architecture of the proposed system. The clinician can submit a recommended treatment regimen, as a set of rules, to the MPCS server, which also receives compliance self-reports gathered from the patient's mobile phone, either using manual inputs or automatic sensing. The users' context information is also periodically inferred and sent to the server, which uses the user context and historical data to determine an optimal reminder delivery schedule. The server also detects non-compliance by comparing the treatment regiment and the self-reports, and triggers a rating questionnaire on the patient's mobile phone. The ratings are used to infer non-compliance reason(s) and the clinician is asked to choose an evidence-based intervention strategy. Family members can also log in to see the patient's health conditions and compliance activities. Patients themselves can interact with their social community through their mobile phones. In particular, they can browse group-level compliance activities of their peers and follow detailed compliance actions of their buddies, as permitted by the privacy settings. Next, we discuss two fundamental challenges in the design and implementation of the MPCS.

A. Power Consumption

The client application on the mobile phone must run continuously to send data from wireless medical sensors or manual inputs, and to receive reminders, questionnaires, and social updates. In particular, the users' location and activities

should be inferred using on-board sensors to build contextual user profiles. Thus power consumption must be carefully considered.

Studies have shown that the battery life can reduce to less than 7 hours if GPS is continuously used (Nokia N95) [16]. To prolong the battery life, researchers have proposed to trade off the localization accuracy by opportunistically using Wi-Fi and GSM-based localization [16], [9]. Activity inference using an embedded accelerometer and audio sensor also consumes non-trivial energy, which may reduce the battery life to less than 6 hours (Nokia N95) [34]. The inference intervals can be enlarged to preserve power, but the inference accuracy will be reduced as a tradeoff.

Emerging off-the-shelf wireless medical sensors often use low-power Bluetooth communications and act in the master mode. To reduce manual input, the Bluetooth-enabled mobile phones constantly probe to discover and connect with nearby sensor devices. The device discovery process may consume 100–200mW energy and take about 10 seconds, depending on the particular Bluetooth devices [12]. Once connected, the medical sensor may either automatically start pushing data to the phone or require some user actions to start data transfer, such as pressing a button on the blood pressure monitor or stepping off the weight scale.[2] Bluetooth supports multiple low-power modes once connected, but a mobile phone acting in the slave mode needs to keep the radio on and perform an inquiry scan before joining a piconet, resulting in non-trivial power consumption [52].

Data transmission over a cellular network also incurs significant energy cost on mobile phones. One possibility to prolong battery life (and reduce network charges) is to opportunistically transfer data using a Wi-Fi network, which is becoming pervasive and often supported by latest smart phones [41]. In addition, it may also be sensible to compress the data to save bandwidth, since local computation often consumes less power than transmission. How to effectively manage several radio interfaces, trade off data compression and bandwidth, and trade off compression with transmission delay, remains as an interesting research problem.

B. Security and Patient Privacy

Medical data collected by the mobile device is extremely personal. It can reveal the patients' dietary habits, daily schedule, disease stage, treatments rendered, medications taken, psychological profiles, and even social relationships. If leaked to the wrong person, it could be devastating to the patients' safety and social life. Without assurance of privacy, patients may resort to lying or omitting details in their reports. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Health Information Technology For Economic and Clinical Health (HITECH) portion of the American Recovery and Reinvestment Act (ARRA) of 2009 require every health provider to comply with its Privacy and Security standards to protect patients privacy and quality of service. To comply with

HIPAA and HITECH rules [20], [28], the health-monitoring system should provide the following security services: data security, entity authentication, access control, auditing, privacy management, and secure data sharing.

a) Key management: Many security services (below) require proper key management. For example, the system should generate, distribute, and revoke secret keys used for data encryption. Because of the computation power available in today's mobile devices, public-key cryptography can provide secure and flexible key management [44]. However, public-key cryptography is known to consume a lot of energy [43]. For longer battery lifetime, energy-efficient public-cryptography [6], [45], [18], [22] and combination of public-and private-key cryptography should be considered.

Trusted Platform Module (TPM) technology [50] can also protect the credentials stored on mobile device from unauthorized access. Although TPMs are currently available only on laptops, desktops, and servers, we expect to see TPMs in mobile devices soon [36].

b) Data security: Data security of health data consists of data confidentiality and data integrity. For data confidentiality, every piece of data should be encrypted before storing it in the device or transmitting it over the network; only the authorized recipient can decrypt and access the data. Although current best practices require AES encryption [44], AES might not be the best choice for encrypting a large amount of stream data in mobile devices with a limited battery lifetime [32]. Therefore, it is worth considering alternatives for better performance and energy conservation for stream-data encryption [24].

Data integrity should be protected with proper message authentication codes (MAC) so that any unauthorized modification of the data can be detected. However, we need different MACs for different purposes. When the patient's data is sent to the health provider, the physician wants to verify that the data is coming from the specified patient and was not modified in transit. When data is shared with peer-group members, the recipient of the data wants to verify that the data is authentic, but should not learn whose data it is. Thus, secure hashing or RSA signatures can serve as an identifiable MAC, while anonymous group signatures [7] can serve as an unidentifiable MAC.

c) Entity authentication: Every person who wants to access patient data needs to be authenticated, both to determine whether they are authorized to view the data, and to provide detailed audit logs of which people access which patient data. A person can access patient data through many different routes, whether from a mobile phone at the grocery store through a 3G cellular network, from a desktop PC at a family member's workplace through an enterprise Internet connection, or from a PDA at doctor's office through an in-hospital wireless network. There are many available authentication methods and one might be more appropriate in a certain situation than another.

An interesting issue is patient authentication. Patient authentication is critical not only because the patient has full access to the data but also because patient authentication

---

[2]http://www.lifesourceonline.com/

is the foundation for data authentication. In other words, improper patient authentication can lead the system to believe that the data is coming from the claimed patient when it is not. For strong patient authentication, a biometric such as fingerprints can be used. However, the use of permanent identifiable biometrics can raise privacy concerns. Moreover, when the patient intends to deceive, the authentication can still fail. Several studies have investigated the use of physiological signals such as the Electrocardiogram (ECG) or Photoplethysmograph (PPG), for patient authentication [3], [5], [2], [19]. The advantage of physiology-based authentication is that it is difficult to decouple the authentication data and the medical data. However, most existing frameworks are unreliable during intense activity and other varied conditions. The challenge in applying these techniques to patients with chronic disease is to support reliable authentication during the course of daily activities.

d) Access Control: Every access to patients' medical data should be authorized and audited. That is, whenever a person attempts to perform an operation on data (e.g., read, change, or delete), the system should verify if the person is actually granted for that operation on that data (called authorization). Furthermore, to comply with the HITECH Act security rules, every access should be recorded and auditable [40]. Since a health-monitoring system has many different groups of people with different roles, an access-control method should be chosen accordingly. Although the role-based access control (RBAC) model [14] seems appropriate for its flexibility in managing various access rights to different people by decoupling entities from roles, and indeed has been selected by standards like Health Level 7 (HL7), it has several limitations. There is no way to express override policies, sometimes called "break-glass" mechanisms, that allow access in the event of an emergency; Motta et al. provide a context-sensitive RBAC approach for electronic patient records [35]. Furthermore, classic RBAC systems were not designed with privacy in mind; more recent work on privacy-aware RBAC may be helpful [37], [38].

e) Anonymous data sharing: To support peer-group data sharing (as proposed in Section III-C), the system should provide an anonymous health-data repository (AHR) service that stores de-identified medical records and generates useful statistics about the progress and compliance status of anonymous patients. The AHR service is designed to be completely unaware of any identifiable data of patients and should guarantee at least a minimum level of anonymity of patients in case of invasion.

Protecting privacy in medical data has been extensively studied [4], [30], [46], [47]. Most work is based on attribute-blurring using hierarchical binning techniques. Attribute-blurring, however, can fail to protect patients' privacy against sophisticated identification attacks, leading to the development of the concept of k-anonymity [48]. Due to its simplicity and general effectiveness, the k-anonymity model revived research on privacy-aware data mining and data release [29], [49], [10], [21], [1]. These techniques may form the foundation of methods to disclose the desired information to peer-group members while protecting desired patient privacy.

In summary, providing system-wide security and privacy guarantees for MPCS is a rich and challenging research area.

V. SUMMARY AND FUTURE WORK

In this position paper we describe a Mobile-based Patient Compliance System (MPCS) for better chronic illness care. Our focus is to address the limitations of the self-regulation approach to facilitate its adoption and improve its effectiveness. The novel contribution is that we use well-grounded social-behavioral theories as the design principles for a system built with pervasive mobile technology (primarily mobile phones), to positively influence patient behaviors by reducing compliance obstacles and improving compliance motivations. Earlier work has been based on paper diaries and periodic patient interviews, whereas we plan to use mobile phones for frequent (perhaps even continuous) monitoring of patient health and compliance, with real-time reporting to the provider and rapid feedback to the patient. Earlier technology-based approaches have been limited to fixed-schedule reminders, whereas we plan to use adaptive reminders based on non-compliance detection and patient context. We are working on an implementation of the proposed system and plan to deploy it with real patients for user studies to validate our hypotheses.

REFERENCES

[1] G. Aggarwal, T. Feder, K. Kenthapadi, R. Motwani, R. Panigrahy, D. Thomas, and A. Zhu. Anonymizing tables. In *Proceedings of the Tenth International Conference on Database Theory*, pages 246–258, 2005.
[2] F. Agraoti and D. Hatzinakos. Fusion of ECG sources for human identication. In *Proceedings of the 3rd International Symposium on Communications, Control and Signal Processing*, page 15421547, Mar. 2008.
[3] E. Bekiaris, I. G. Damousis, and D. Tzovaras. Unobtrusive multi-modal biometric authentication: The HUMABIO project concept. *EURASIP Journal on Advances in Signal Processing*, 2008.
[4] E. Bertino, B. C. Ooi, Y. Yang, and R. H. Deng. Privacy and ownership preserving of outsourced medical data. In *Proceedings of the 21st IEEE International Conference on Data Engineering*, pages 521–532, 2005.
[5] L. Biel, O. Pettersson, L. Philipson, and P. Wide. ECG analysis: A new approach in human identication. In *Proceedings of the 16th IEEE Instrumentation and Measurement Technology Conference*, 1999.
[6] I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic curves in cryptography.* Cambridge University Press, 1999.
[7] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *Proceedings of Crypto*, pages 41–55, 2004.
[8] S. W. Campbell and T. C. Russo. The social construction of mobile telephony. *Communication Monographs*, 70(4), 2003.
[9] I. Constandache, S. Gaonkar, M. Sayler, R. R. Choudhury, and L. Cox. Enloc: Energy-efficient localization for mobile phones. In *Proceedings of the 28th Conference on Computer Communications*, Rio de Janeiro, Brazil, Apr. 2009.
[10] L. Cox. Suppression methodology and statistical disclosure control. *J. American Statistical Association*, 75:377–385, 1980.
[11] A. M. Delamater. Improving patient adherence. *Clinical Diabetes*, 24(2):71–77, 2006.
[12] A. Devlic, A. Graf, P. Barone, A. Mamelli, and A. Karapantelakis. Evaluation of context distribution methods via Bluetooth and WLAN: Insights gained while examining battery power consumption. In *Proceedings of the International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous)*, Dublin, Ireland, July 2008.

[13] F. Evangelista, G. Albaum, and P. Poon. An empirical test of alternative theories of survey response behavior. *Journal of the Market Research Society*, 41(2):227–244, Apr. 1999.

[14] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli. Proposed nist standard for role-based access control. *ACM Trans. Inf. Syst. Secur.*, 4(3):224–274, 2001.

[15] J. Fulk. Social construction of communication technolog. *Academy of Management Journal*, 36(5), 1993.

[16] S. Gaonkar, J. Li, R. R. Choudhury, L. Cox, and A. Schmidt. Micro-blog: sharing and querying content through mobile phones and social participation. In *Proceedings of the The International Conference on Mobile Systems, Applications, and Services (MobiSys)*, pages 174–186, Breckenridge, CO, June 2008.

[17] V. Gay and P. Leijdekkers. A health monitoring system using smart phones and wearable sensors. *International Journal of Assistive Robotics and Mechatronics*, 8(2):29–36, June 2007.

[18] J. Goodman, A. P. Chandrakasan, and A. P. Ch. An energy-efficient reconfigurable public-key cryptography processor. *IEEE Journal of Solid-State Circuits*, 36:1808–1820, 2001.

[19] Y. Gu, Y. Zhang, and Y. Zhang. A novel biometric approach in human verication by photoplethysmographic signals. In *Proceedings of the 4th Annual IEEE Conference on Information Technology Applications in Biomedicine*, pages 13–14, Apr. 2003.

[20] HIPAA security standard. Federal Register, Feb. 2003. Department of Health and Human Services.

[21] V. S. Iyengar. Transforming data to satisfy privacy constraints. In *Proceedings of the ACM International Conference on Knowledge Discovery and Data Mining*, pages 279–288, 2002.

[22] Q. Jing, J. Hu, and Z. Chen. C4W: An energy efficient public key cryptosystem for large-scale wireless sensor networks. *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference*, pages 827–832, 2006.

[23] A. Jurik, J. Bolus, A. Weaver, B. Calhoun, and T. Blalock. Mobile health monitoring through biotelemetry. In *Proceedings of the Fourth International Conference on Body Area Networks*, Los Angeles, CA, Apr. 2009.

[24] H. Kim, J. Han, and S. Cho. An efficient implementation of RC4 cipher for encrypting multimedia files on mobile devices. In *Proceedings of the 2007 ACM symposium on Applied computing*, pages 1171–1175, 2007.

[25] H.-S. Kim and H.-S. Jeong. A nurse short message service by cellular phone in type-2 diabetic patients for six months. *Journal of Clinical Nursing*, 16(6):1082–1087, May 2007.

[26] O. Kwon and S. Choi. Applying associative theory to need awareness for personalized reminder system. *Expert Systems with Applications*, 34(3):1642–1650, Apr. 2008.

[27] H. Leventhal, E. Halm, C. Horowitz, E. A. Leventhal, and G. Ozakinci. Living with chronic illness: A contextualized, self-regulation approach. In *The SAGE Handbook of Health Psychology*. SAGE Publications Ltd., 2004.

[28] C. A. Leyva and D. L. Leyva. HIPAA survival guide for providers: Privacy & security rules. http://www.hipaasurvivalguide.com/, 2009.

[29] J. Li, W. Hua, H. Jin, and J. Yong. Current developments of k-anonymous data releasing. *Electronic Journal of Health Informatics*, 3(1), Mar. 2008.

[30] Z. Lin, M. Hewitt, and R. Altman. Using binning to maintain confidentiality of medical data. In *Proceedings of the American Medical Informatics Association Annual Symposium*, pages 454–458, 2002.

[31] A. G. Logan, W. J. McIsaac, A. Tisler, M. J. Irvine, A. Saunders, A. Dunai, C. A. Rizo, D. S. Feig, M. Hamill, M. Trudel, and J. A. Cafazzo. Mobile phonebased remote patient monitoring system for management of hypertension in diabetic patients. *American Journal of Hypertension*, 20(9), 2007.

[32] C. Mathur and K. Subbalakshmi. Nis05-5: Energy efficient wireless encryption. In *Proceedings of the Global Telecommunications Conference*, pages 1–5, Dec. 2006.

[33] J. C. McElnay, C. R. McCallion, F. Al-Deagi, and M. Scott. Self-reported medication non-compliance in the elderly. *European Journal of Clinical Pharmacology*, 53(3–4):171–178, Dec. 1997.

[34] E. Miluzzo, N. D. Lane, K. Fodor, R. Peterson, H. Lu, M. Musolesi, S. B. Eisenman, X. Zheng, and A. T. Campbell. Sensing meets mobile social networks: The design, implementation and evaluation of the CenceMe application. In *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems (SenSys)*, Raleigh, NC, Nov. 2008.

[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*, 7(3):202–207, Sept. 2003.

[36] Mobile Phone Work Group. Web site visited in May 2009.

[37] Q. Ni, D. Lin, E. Bertino, and J. Lobo. Conditional privacy-aware role based access control. In *Proceedings of the 12th European Symposium On Research In Computer Security (ESORICS)*, volume 4734, pages 72–89. Springer-Verlag, Sept. 2007.

[38] Q. Ni, A. Trombetta, E. Bertino, and J. Lobo. Privacy-Aware Role Based Access Control. In *Proceedings of the 12th ACM Symposium on Access Control Models and Technologies (SACMAT)*, pages 41–50. ACM Press, June 2007.

[39] N. Oliver and F. Flores-Mangas. Healthgear: A real-time wearable system for monitoring and analyzing physiological signals. In *Proceedings of the International Workshop on Wearable and Implantable Body Sensor Networks*, pages 61–64, Los Alamitos, CA, USA, 2006.

[40] L. Peyton, C. Doshi, and P. Seguin. An audit trail service to enhance privacy compliance in federated identity management. In *Proceedings of the Conference of the Center for Advanced Studies on Collaborative Research*, pages 175–187, 2007.

[41] A. Rahmati and L. Zhong. Context-for-wireless: Context-sensitive energy-efficient wireless data transfer. In *Proceedings of the The International Conference on Mobile Systems, Applications, and Services (MobiSys)*, pages 165–178, San Juan, Puerto Rico, June 2007.

[42] R. A. Rescorla and A. R. Wagner. A theory of pavlovian conditioning: Variations in the effectiveness of reinforcement and non-reinforcement. In *Classical Conditioning II. Current Research and Theory*, pages 64–99. Appleton Century Crofts, 1972.

[43] N. Ruangchaijatupon and P. Krishnamurthy. Encryption and power consumption in wireless LANs. In *Proceedings of the 3rd IEEE Workshop on Wireless LANs*, 2001.

[44] B. Schneier. *Applied Cryptography*. John Wiley & Sons, 1996.

[45] M. Shand and J. Vuillemin. Fast implementations of rsa cryptography. In *Proceedings of the 11th Symposium on Computer Arithmetic*, pages 252–259, June 1993.

[46] L. Sweeney. Datafly: A system for providing anonymity in medical data. In *Proceedings of the International Conference on Database Security*, pages 356–381, 1997.

[47] L. Sweeney. Guaranteeing anonymity when sharing medical data, the Datafly system. In *Proceedings of the American Medical Informatics Association Annual Symposium*, pages 51–55, 1997.

[48] L. Sweeney. K-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5):557–570, 2002.

[49] K. Tan, J. Yeo, M. E. Locasto, and D. Kotz. Catch, clean, and release: A survey of obstacles and opportunities for network trace sanitization. In F. Bonchi and E. Ferrari, editors, *Privacy-Aware Knowledge Discovery: Novel Applications and New Techniques*. Chapman and Hall CRC Press, February 2009. Under review.

[50] Trusted Platform Module. Web page visited May 2009.

[51] E. H. Wagner, B. T. Austin, C. Davis, M. Hindmarsh, J. Schaefer, and A. Bonomi. Improving chronic illness care: Translating evidence into action. *The Policy Journal of the Health Sphere*, 20(6), 2001.

[52] C.-Y. Wan and S. Prasad. Challenges to building bluetooth-based sensing solutions. In *Proceedings of the Fourth International Conference on Body Area Networks*, Los Angeles, CA, Apr. 2009.

[53] Adherence to long-term therapies: Evidence for action. World Health Organization Report, 2003.