Authentication and Usability in mHealth Apps

Zhongwei Teng, Peng Zhang, Xiao Li, William Nock, Marcelino Rodriguez-Cancio,
Denis Gilmore, Jules White, Douglas C. Schmidt, Jonathan C. Nesbitt
Vanderbilt University, Nashville, Tennesse, USA
Email: zhongwei.teng@vanderbilt.edu

***Abstract*—Mobile health (mHealth) apps have been adopted in areas of healthcare such as the management of diabetes, monitoring physical activities and the treatment of HIV. This paper provides three contributions to research on how the usability of an mHealth app impacts its frequency of use and adoption. First, we evaluate how different authentication approaches for mHealth apps impact their usability. Second, we present new metrics for evaluating mHealth app usage complexity in the context of four potential barriers to use: memory barriers, physical barriers, process barriers, and other barriers. Third, we evaluate the usability of two common authentication approaches for mHealth apps via several key process aspects and their impact on users. Based on the results, we propose a QR-Code based authentication approach for mHealth apps, which help overcome common impediments faced by mHealth apps that are used in acute care and other settings.**

***Index Terms*—mHealth, Authentication, Evaluation**

I. Introduction

Emerging trends & challenges. The rapid adoption of mobile devices has generated significant interest in using mobile health (mHealth) apps to support traditional healthcare research. These apps have been widely adopted in chronic condition monitoring, remote patient monitoring and disease treatment, such as HIV treatment [1], testing, and data collection [2]. Combining mHealth techniques with other interventions may improve overall care [3].

Ensuring security and privacy are key challenges to address in any mobile technology. In mHealth apps, patients' sensitive data must be protected carefully. For example, mHealth apps may store users' daily activities and even sleeping patterns [4] in mobile devices, where private data might be collected by Android advertising networks[5]. To protect sensitive information, rigorous authentication and security mechanisms, such as data-at-rest and data-in-transit encryption, must be applied.

Cyber-physical identity (CPI) linkage connects a patient's digital identity in a medical record system (e.g., master patient identifier, etc.) to a physical mobile device. This linkage is a vital process for accurately and securely collecting medical data for a patient. For example, a mismatched identity could cause incorrect information sent from a mobile device to enter the wrong patient record and impact treatment decisions, such as prescribing opioids to the wrong patient. The CPI linkage process is akin to checking arm bands to ensure that the correct person is linked to a medical record, though in the case of CPI linkage patient records are linked to mobile device(s) that report health information related to that patient.

To ensure security and identify validation, many authentication methods use complex workflows. For mHealth apps, however, ensuring ease of use is essential since users are often (1) *sick patients*, who have limited mental and physical resources or (2) *nurses and providers*, who have limited time and already must follow complex processes. According to Marie-pierre Gagnon[6], usability has been shown to directly impact the frequency of use and adoption of mHealth apps.

Key contributions. This paper presents an analysis of how varying authentication and CPI establishment architectures impact the usability of mHealth apps for patients and providers. In particular, we explore a method for evaluating authentication methods of mHealth apps in the context of patient and provider burdens. We then evaluate two conventional approaches—username/password and SMS based authentication—in the context of several key process aspects. Based on the results of this evaluation we propose a third method—QR-Code token transfer and authentication—that is designed to overcome limitations of conventinal approaches.

This paper provides several contributions to the study of authentication approaches in mHealth apps, including (1) discussing how conventional mHealth app authentication and account linkage schemes incur burdens on providers and patients, (2) providing evaluation metrics for authentication and CPI linkage in mHealth apps, (3) evaluating two widely used authentication methods and describing limitations with these approaches, and (4) proposing a solution using QR-Codes to transfer authentication tokens to overcome potential challenges of existing methods.

Paper organization. The remainder of this paper is organized as follows: Section II presents a motivating example, the PainCheck app, that is used throughout the paper; Section III discusses some key process aspects of authentication methods in mHealth apps that must balance usability and security; Section IV summarizes different usability and process barriers that impede the adoption of mHealth apps and proposes evaluation methods for assessing them; Section V analyzes two widely used authentication approaches and a proposed authentication method using QR codes and authentication tokens; Section VI compares and contrasts our research with related work on mHealth security; and Section VII presents concluding remarks and outlines future work.

II. Motivating Example

For decades, pain monitoring has played a critical role in healthcare. Evidence extracted from published data shows that "concise postoperative pain measurement has a comparable positive influence to the pain management strategy" [7]. The

measurement of subjective pain intensity is important to both researchers and clinicians [8] and can aid in determining appropriate dosage of pain medications.

This paper uses the PainCheck mHealth app as a motivating example. PainCheck was developed at Vanderbilt University using the ReactNative platform (which runs on both iOS and Android) to help patients report their pain levels following thoracic surgery in both acute and post-acute settings. Figure 1 shows screenshots of the app. Immediately following

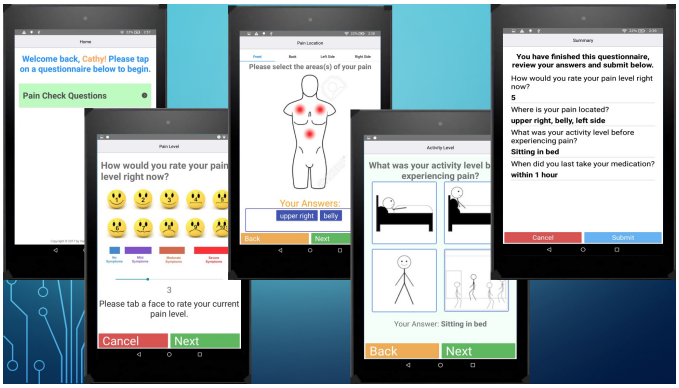

Fig. 1. Screenshots of the PainCheck app

surgery, nurses, patients, and care-givers can use PainCheck to report subjective pain levels for a patient suffering from post-operative pain. Patients and care-givers can report pain scores both in the hospital and after leaving for a configurable period of time.

III. Key Process Aspects to Consider

When patients use the PainCheck app to report their pain, authentication is required to ensure data entries are matched to the correct patients. This section examines existing authentication methods to gain insight into how they may affect the usability of mHealth apps. Below we describe key process steps, such as credential transfer and cyber-physical linkage, which must be considered in any data collection process.

1) Credential transfer to users: Traditional paper-based approaches to collecting data rely on physically creating a piece of paper with the patient's identity (or asking them to fill it in) and giving this piece of paper to the patient or caregiver to collect patient information. For a cyber-based data collection approach, such as a mobile app, an account must be created with security credentials used to protect access to the account. Moreover, similar to the paper-based data collection method, a patient or caregiver must be given these account security credentials to submit data into the account, similarly to how the physical paper must be given to the patient so that they can submit data about themselves.

All data collection approaches must support the creation of an account for the patient and the transfer of authentication credentials to the patient. This credential transfer process is a critical step to consider since it places a burden on both nurses and patients. For example, nurses expend time and energy acquiring, protecting, and communicating the credentials to the patient. Likewise, patients must be able to receive the credentials without error. The security approaches we analyze in Section V use different processes to perform this transfer, which have a direct impact on how error-prone and time-consuming this transfer may be.

2) Cyber-physical Identity (CPI) linkage of mobile devices: To collect valid data from patients, mobile device(s) must be linked with a patient's identity through a CPI linkage. For example, a tablet in the patient's room that is owned by the hospital, a mobile phone owned by the patient, and a mobile phone owned by a patient's guardian may all be linked to the patient's account so that a nurse, the patient, or the guardian can submit pain data on behalf of the patient. Each security architecture has different processes for linking new physical devices to a CPI that impact patient and provider complexity and time.

3) Credential entry on physical devices: After a patient has received authentication credentials, they typically must enter the credential fields into a mobile device to be authenticated. For example, if a patient is given a username/password, they must type these fields into a device in order to authenticate their account, allowing them to submit data on their behalf. Likewise, authentication processes normally require re-entry of such credentials at some frequency in order to maintain access.

The complexity of the credentials that a security architecture imposes on patients, as well as the frequency with which they must be entered, places a burden on the patient, caregivers, and providers. For example, requiring patients to use randomly-generated passwords with many numbers, symbols, and mixes of character case may increase security at the expense of making it more difficult for patients to enter the credential onto their device. Conversely, allowing patients to choose their own passwords simplifies their data entry at the expense of requiring nurses to orchestrate account creation and password collection from patients.

4) Credential loss & recovery: Credential loss is common for mHealth app users. Patients suffering pain significant enough it impair their memory and concentration are likely to forget their authentication credentials. When a patient forgets or loses their credentials, a credential recovery or reset process is needed. Regardless of how the reset is performed, this process places additional burdens on patients and staff.

IV. Evaluation Criteria

To understand how mHealth cyber-physical linkage and authentication approaches impact usability, we developed a series of evaluation metrics. This section examines several types of usage impediments present in different authentication approaches. By describing these impediments, we help researchers understand how an mHealth authentication method impacts patients and providers.

A. Memory Impediments

A memory impediment is a requirement for a patient to remember a specific set of information. This information can

be a username/password or a process that must be followed. Remembering a long string of account/password characters can be hard for patients that are already in pain. Even healthy people, however, rarely change their passwords and tend to use the same passwords among various services due to the challenge of learning and remembering new passwords. A survey conducted by Telesign [9] revealed that 21% and 47% of people use 5-year old and 10-year old passwords, respectively. Moreover, 70% of customers show concern about their account security, but 73% of accounts still use the same password, which is highly vulnerable to attack since hackers only need to obtain access to one password to attack other accounts of the same owner.

We define the following metrics to measure the memory and recall burden placed on a patient relative to the security of the underlying authentication credential: **M1. Total characters remembered relative to credential length** and **M2. The duration that patients need to remember the data relative to length of treatment**.

We use these metrics to ascertain how much a patient must remember relative to the security of the underlying credential. Some processes require patients to remember the complete security credential. A patient must therefore remember as many characters as are in the underlying security credential used to authenticate, or O(n) characters, where "n" is the length of the security credential.

As shown in Section V, other authentication approaches only require the patient to remember a one-time password that is then exchanged by the device for an authentication token that can be much more complex than the original password. In this case, the authentication credential and the password are decoupled since after the first use the token is used to authenticate and need not be remembered by the patient. The total characters remembered by the patient is thus O(1) since the length of the one-time password is constant and independent of the length of the underlying security token. As with algorithmic complexity analysis, authentication approaches that require patients to remember O(1) characters are typically better than approaches that require O(n) characters.

B. Physical Impediments

Physical impediments are operations a patient must perform during the authentication process, including pressing on the device, typing on the device, or shaking the device. According to a survey in 2003 [10], elderly patients age 65 and older constitute one third of hospital stays. Eyesight, senility, and postoperative fatigue are common problems in elderly patients and can impact data entry on mobile devices. Moreover, typos happen more frequently on mobile devices compared to typing on a keyboard and typing on a small screen is slower for most people, particularly those with age-related motor control issues or surgery-related health issues.

mHealth apps need to minimize these physical impediments to facilitate use. An ideal authentication method should reduce these impediments to improve user experience while maintaining equivalent security. We therefore propose following two measures of physical impediments that we leverage to assess mHealth authentication approaches: **Ph1. Total characters typed relative to credential length** and **Ph2. Total characters typed for credential recovery relative to credential initialization**.

Similar to the memory impediments, we measure physical impediments in terms of how much typing a patient must perform relative to the length of the underlying security credential. Better authentication approaches for mHealth apps allow the length of the underlying security credential to vary independent of how much data a patient enters.

C. Process Impediments

Process impediments capture the complexity and potential errors inherent to an mHealth authentication architecture. For example, when nurses treat a number of patients each day, a long repetitive account setup process can yield mistakes, such as giving the wrong authentication credentials to a patient, causing them to submit pain data to the wrong patient record. Process barriers can be analyzed by calculating the total process steps for both providers and patients. We measure process impediments in terms of the following steps: **P1. Total process steps for provider**, **P2. Total process steps for patients**, and **P3. Total error-prone steps**.

D. Other Impediments

Other impediments incur additional demands, such as cost and hardware usage, that are unique to a specific approach. For example, the SMS authentication system discussed in Section V requires the device being signed into to have cellular service, as well as a network connection, whereas other approaches do not require cellular service.

V. Techniques Evaluated

This section describes how we evaluated several identication and CPI linkage approaches using the criteria covered in Section IV. As shown in Sections sec:usr and sec:sms below, two of these approaches (username/password and SMS-based authentication) incur significant impediments and burdens on patients and providers. Section V-C describes how we applied QR-Codes and authentication tokens to address these challenges for the PainCheck mHealth app.

A. Username/password

Username-password authentication is a widely used authentication method. A verification table stores usernames and hashed passwords. Clients are authenticated by providing a username and a password that is checked against the stored table of account credentials. After providing correct information, mHealth apps can then take actions on the data in that account, such as sending pain information to the server.

Credential transfer to users. Doctors only want patients who are actively receiving treatment to submit pain data to the PainCheck app, thereby avoiding invalid data from arbitrary users. Providers thus need to control account creation and physical identity establishment. To link a new device to

TABLE I
EVALUATION OF AUTHENTICATION METHODS

	Metrics	Username/password	SMS+OTP	QR+OTP
M1	Total characters remembered relative to credential length	O(n)	O(1)	O(1)
M2	The duration that patients need to remember the data relative to length of treatment	O(n)	O(1)	O(1)
Ph1	Total characters typed relative to credential length	O(n)	O(1)	O(1)
Ph2	Total characters typed for credential recovery relative to credential initialization	O(n)	O(1)	O(1)
P1	Total process steps for provider	4	2	1
P2	Total process steps for patient	2	1	1
P3	Total error-prone steps	4	2	1
	Binary Metrics			
O1	Additional costs / Barriers	NO	Cellular Service, SMS Charges	NO

the patient's PainCheck account, a provider must create a username/password for the patient and/or coordinate collecting a username/password from the patient to create the account. Either way, a coordination step must occur to collect or distribute a username/password to/from a patient, as shown in steps 1-4 of Figure 2.

Table I applies the metrics from Section IV to username/password authentication. The total characters remembered and typed relative to credential length is O(n) since patients must remember their entire username/password to login to a device. The duration that patients will need to remember the data is the length of the treatment period, which is O(n).

Cyber-physical identify (CPI) linkage of mobile devices. To link a new physical mobile device to a patient's account, the username/password credentials for the patient or for an account that has access to that patient's data must be entered onto that device. Providers must manage this CPI linkage process since patients must be signed up without problems and the linkage must be performed accurately.

Table I shows the evaluation of metrics P1-3 for this process. Providers must perform a total of four steps: create the credential, link identities, print accounts, and give accounts to the patients. Patients must enter the username/password on their device. Error-prone steps include (1) providers incorrectly linking patient accounts to mobile devices (e.g., linking the wrong device and account), (2) providers incorrectly transferring account credentials to patients (e.g., giving the wrong password to the patient), and (3) entering incorrect usernames/passwords into the device.

Credential entry on physical devices. After obtaining username/password credentials from a provider, patients or caregivers must manually enter the credentials on a mobile device. Since initial passwords are normally generated randomly (which may include letters, numbers, or special characters), it will take longer for patients to enter credentials compared to if they choose their own custom passwords. The overall security of the password is usually much stronger, however, if a random password is generated for the patient since human-produced passwords are prone to dictionary and other attacks. Regardless of the approach, the total number of characters that must be typed on the mobile device is proportional to the length of the security credential (i.e., O(n)), as shown in metrics Ph1 in Table I.

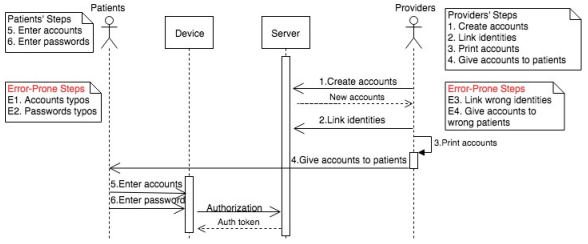

Fig. 2. Diagram of Username/Password Authentication

Credential loss & recovery. In the event that a patient or caregiver forgets their username/password, a credential recovery process must be followed, such as having a provider reset the patient's credentials using an administrative account or emailing a password reset link to the patient. Regardless of the approach, the patient and/or provider must remember and enter data proportional to the length of the new credential into the system, which requires typing O(n) characters, as shown in metric Ph2 in Table I.

B. SMS-based Authentication

A limitation of username/password authentication on mobile devices is that patients or caregivers must initially type a long password into their device. As shown by the prior evaluation of the memory, process, and data entry metrics in Section IV, transferring the initial credential to the patient and typing it into the device incurs an additional burden on the patient.

An alternative approach is to use a combination of a *one-time password* (OTP) and short-message service (SMS) distribution of the OTP. This approach generates a user account and then generates OTPs to link a device to an account, as shown in Figure 3. To link a device to an account, a provider specifies the cell number of the desired device to link and a unique OTP is generated and sent to the device via SMS. The SMS can encode the OTP in a link that a patient can click to automatically transfer the OTP into the app (e.g., a custom iOS URI scheme).

After an mHealth app on the device receives the OTP, it sends the OTP to the server. The server then validates the credential, determines the account it is attached to, and sends an authentication token back to the device/app for use in future authentications. This approach simplifies the transfer of the

initial credential to patients and eliminates the need for patients to manually type credentials into the device.

Credential transfer to patients. After creating an account, providers need to link a phone number with the new account. Credentials can then be transfered to patients via SMS. Table I applies the metrics from Section IV to the SMS-based authentication approach. The credential saved in the device can be more complex than the OTP (which is usually a 5-8 digit code), so the total characters remembered and typed as a function of credential length is O(1).

The duration that patients need to remember the data is not related to the length of treatment since patients need not remember OTPs and the authentication tokens are automatically remembered and managed by the app, which yields O(1) for the total characters remembered. As shown in Table I, however, SMS-based authentication has additional impediments. For example, applying SMS-based authentication requires mobile devices to have cellular service and requires providers to pay SMS messaging charges.

Cyber-physical identity (CPI) linkage of mobile devices. CPI linkage occurs when the provider specifies which telephone number to send the OTP to. For this linkage approach to work, patients must provide their phone numbers, which are used as the identity of the mobile device. If the provider selects the incorrect account or sends the OTP to the wrong telephone number, an incorrect linkage can occur or the wrong individual can be given access to an account (e.g., the OTP is sent via SMS to the wrong phone number).

Table I shows the evaluation of metrics P1-3 for this process. Providers have two steps: (1) generating new accounts and (2) sending the OTP for the patient to the correct phone number(s). Patients only have one step: clicking the link in the SMS. The only error-prone steps during the authentication are that providers must select the correct patient within the system (e.g., avoid selecting a patient with the same name but a different birthday) and send the SMS messages to the correct phone number(s) (e.g., a typo in the phone number could send the OTP to a random person).

Credential entry on physical devices. Since the OTP is sent as a link in an SMS that can transfer the OTP into the app automatically, patients need not type the credentials into the device. As shown in metric Ph1, the total number of characters that must be typed on the mobile device is not related to the length of the security credential (O(1)).

Credential loss & recovery. Credential loss cannot occur with an SMS approach since the mHealth app manages the authentication tokens and remembers them automatically. The only risk is that a provider sends the OTP to the wrong phone number initially. After the OTP is exchanged for an authentication token, the token is remembered automatically by the app, thereby eliminating credential loss issues.

C. QR-Code based Authentication

A key benefit of the SMS + OTP approach is that it improves mHealth app ease of use by eliminating manual entry of the initial credential and automating the transfer of credentials.

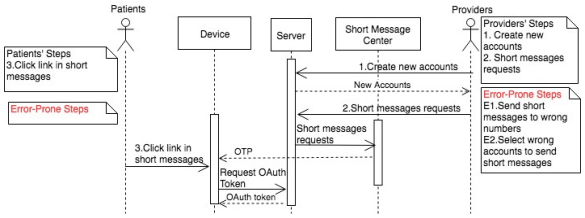

Fig. 3. Diagram of SMS-based Authentication

This approach, however, incurs several downsides. First, it requires the patient and provider have a telephone number (e.g., an Internet connected device is insufficient) and they must have cellular coverage in the patient room (e.g., to allow the patient to link their device). Second, the approach has the potential for errors if OTPs are sent to the wrong phone number.

To overcome these limitations, we designed an alternative authenticaion approach that combines OTPs with transfer via QR-Codes. With this approach, OTPs are generated for each device, as shown in Figure 4. Rather than sending the OTPs via SMS, however, the OTPs are encoded into a QR-code that can be displayed on a provider-controlled mobile device or printed on a sheet of paper.

A provider takes the QR-code to the patient or caregiver, who can use the camera on their mobile device to scan it and transfer it to the device/app. This approach maintains the advantages of the SMS OTP approach, i.e., automatic transfer of the authentication credential to the app/device, while eliminating the requirement for a cellular connection and the potential that the OTP is accidentally sent to the wrong device. Only devices physically near the provider that can see the QR-code displayed on the provider's mobile device or printed sheet of paper can possibly receive the OTP.

Hospitals already have extensive physical security mechanisms in place. Since the transfer of the OTP via QR-code requires the physical presence of potential receivers the transfer is more secure and aided by existing hospital security procedures. Even if the QR-code is printed on a sheet of paper that is taken outside of the hospital and lost, the OTP cannot be reused after its initial use (e.g., it is a one-time code) and can be time-limited to protect against lost (e.g., becomes invalid three hours after generation).

Credential transfer to patients. To link a device to a patient's account, the provider generates a QR-code with an OTP embedded within it. After scanning the given QR-Code (which can contain up to 7,089 characters for the OTP), the patient's mobile device automatically transfers the OTP to the app. Both the total characters remembered as a function of credential length and the duration that patients will need to remember the data is O(1) since the patient does not need to remember any credentials at all, as shown in Table I.

CPI linkage of mobile devices. Table I shows the evaluation of metrics P1-3 for this linkage process. Providers must only choose the correct patient to generate the QR code for, as shown in Step 1 of Figure 4. Likewise, patients must only scan the QR-code, as shown in Step 2. The main errors that

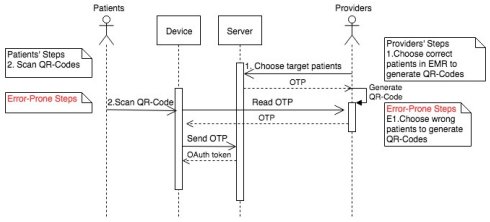

Fig. 4. Diagram of QR-Code based Authentication

can occur are selecting the wrong patient to generate a QR-code for or showing the wrong QR-code to the patient.

Credential entry on physical devices. The credential transfer is automated and the total characters typed relative to credential length is O(1), as shown in Metric Ph1.

Credential loss & recovery. As with SMS+OTP, credentials are automatically remembered by the mHealth app and credential loss is not possible.

VI. Related Work

This section compares and contrasts our research with related work on mHealth security. In studies of authentication in mHealth, prior work focuses on improving the resistance of an authentication method to attacks from malicious third parties by optimizing authentication protocols and encryption schemes [11, 12]. Attacks from the outside, however, are not the only threat that must be dealt with for mHealth. In particular, Kotz et al. have categorized privacy-related threats in mHealth systems [13], which can be caused by not only malicious third parties but also service providers and patients (inside threats). For example, patients themselves could share their credentials that can then be used by others.

The impact of security on usability [6] is not widely studied by mHealth authentication researchers. This paper complements existing authentication literature by defining metrics for analyzing burdens that authentication processes place on patients and providers and shows how different authentication processes lessen these burdens without impacting security.

VII. Concluding Remarks

This paper evaluated a set of mHealth authentication techniques to determine (1) how they impact clinical workflows and (2) what types of burdens they place on patients and providers. We also presented several metrics that can be used to quantify the burdens that authentication mechanisms place on patients and providers, including the amount of information that patients must remember and the number of steps that are added to a clinical workflow. In general, different authentication techniques have steps of roughly the same complexity, though there is wide variation across authentication approaches in terms of the total number of steps, amount of information that patients must remember, and types of errors.

Based on the research conducted in this paper, we learned the following lessons that are relevant for researchers evaluating how the usability of an mHealth app impacts its frequency of use and adoption:

- Username/password authentication approaches are not ideal for mHealth apps in acute care settings. Barriers in Section IV bring potential usage problems to patients.
- Combining SMS with OTPs significantly reduces the burdens on patients and providers, but introduces the requirement that all patients have cellular service on a device and creates the significant potential that a patient's authentication credentials might accidentally be sent to the wrong person.
- The QR-code + OTP method described in Section V preserves the key usability improvements of SMS + OPT authentication, but eliminates the requirement for cellular service and the potential of sending credentials to the wrong person.

In future work we are extending our research to outpatients so that mHealth apps like PainCheck can provide patients with highly usable authentication methods even for patients who are not in a hospital.

Bibliography

[1] Carole Leach-Lemens, JA Blaya, HS Fraser, et al. Using mobile phones in hiv care and prevention. *HIV and AIDS Treatment in Practice*, 137, 2009.

[2] Caroline Free, Gemma Phillips, Lambert Felix, Leandro Galli, Vikram Patel, and Philip Edwards. The effectiveness of m-health technologies for improving health and health services: a systematic review protocol. *BMC research notes*, 3(1):250, 2010.

[3] Alain B Labrique, Lavanya Vasudevan, Erica Kochi, Robert Fabricant, and Garrett Mehl. mhealth innovations as health system strengthening tools: 12 common applications and a visual framework. *Global Health: Science and Practice*, 1(2):160–171, 2013.

[4] Beenish M Chaudhry. Sleeping with an android. *mHealth*, 3, 2017.

[5] Soteris Demetriou, Whitney Merrill, Wei Yang, Aston Zhang, and Carl A Gunter. Free for all! assessing user data exposure to advertising libraries on android. In *NDSS*, 2016.

[6] Marie-pierre Gagnon. A systematic review of factors associated to m-health adoption by health care professionals. In *Medicine 2.0 Conference*. JMIR Publications Inc., Toronto, Canada, 2014.

[7] SJ Dolin, JN Cashman, and JM Bland. Effectiveness of acute postoperative pain management: I. evidence from published data. *British journal of anaesthesia*, 89(3):409–423, 2002.

[8] Mark P Jensen, Paul Karoly, and Sanford Braver. The measurement of clinical pain intensity: a comparison of six methods. *Pain*, 27(1):117–126, 1986.

[9] TeleSign. Telesign consumer account security report. https://www.telesign.com/wp-content/uploads/2015/06/TeleSign-Consumer-Account-Security-Report-2015-FINAL.pdf.

[10] C Allison Russo and Anne Elixhauser. Hospitalizations in the elderly population, 2003. 2006.

[11] Chin-I Lee and Hung-Yu Chien. An elliptic curve cryptography-based rfid authentication securing e-health system. *International Journal of Distributed Sensor Networks*, 11(12):642425, 2015.

[12] Qi Jiang, Xinxin Lian, Chao Yang, Jianfeng Ma, Youliang Tian, and Yuanyuan Yang. A bilinear pairing based anonymous authentication scheme in wireless body area networks for mhealth. *Journal of medical systems*, 40(11):231, 2016.

[13] David Kotz. A threat taxonomy for mhealth privacy. In *Communication Systems and Networks (COMSNETS), 2011 Third International Conference on*, pages 1–6. IEEE, 2011.