










AUTHENTICATION & INTEGRATION APPROACHES FOR MHEALTH APPS FROM A USABILITY VIEW

Zhongwei TENG¹ , Peng ZHANG² , Xiao LI¹ , William NOCK¹ ,
Denis GILMORE³ , Marcelino RODRIGUEZ-CANCIO¹ , Jules WHITE¹ ,
Jonathan Carl NESBITT³ , Douglas Craig SCHMIDT¹ 

¹Department of Electrical Engineering and Computer Science, School of Engineering, Vanderbilt University, 2201 West End Ave, TX 79968 El Paso, Texas, United States of America

²Department of Mathematics and Computer Science, Belmont University, 1900 Belmont Blvd, TX 79968 El Paso, Texas, United States of America

³Department of Thoracic Surgery, Vanderbilt University Medical Center, 1211 Medical Center Dr, TX 79968 El Paso, Texas, United States of America

nzhongwei.teng@vanderbilt.edu, danakzhang@gmail.com, xiao.li@vanderbilt.edu, william.nock@vanderbilt.edu, denis.gilmore@hcahealthcare.com, marcelino.riguez.cancio@gmail.com, jules.white@gmail.com, jon.nesbitt@vanderbilt.edu, d.schmidt@vanderbilt.edu

DOI: 10.15598/aeer.v19i1.3301

Article history: Received Nov 11, 2019; Revised Nov 12, 2020; Accepted Feb 18, 2021; Published Mar 31, 2021. This is an open access article under the BY-CC license.

Abstract. *Mobile Health (mHealth) apps are increasingly adopted in healthcare domains, such as diabetes management, physical activity monitoring, and HIV treatment. However, mHealth app development is restricted due to healthcare privacy regulations, which require apps to handle collected data securely. The advent of online platforms, such as REDCap, alleviates this problem by providing privacy-compliant databases, so that mHealth apps developed for research groups can securely handle stored inactive data (data-at-rest) with fewer privacy concerns.*

Unfortunately, the authentication architectures of many online platforms do not meet the needs of mHealth apps and provide insufficient integration support. Assumptions made in other types of mobile apps about how users operate, such as a user's ability to type or remember a password, therefore may not be valid in the mHealth domain.

To address these problems this paper evaluates how authentication approaches impact the usability of mHealth apps. In particular, we present metrics to evaluate usability and show how the Proxy User Adapter pattern can integrate usability-enhanced authentication approaches to legacy secure database providers. We also propose a QR-Code authentication approach that applies the Proxy User Adapter pattern to help mHealth apps overcome common impediments,

improve processing efficiency, and reduce potential mistakes caused by patients and providers alike.

Keywords

Authentication, mHealth, patterns, usability.

1. Introduction

Emerging trends & challenges. The advent of mobile devices has spurred development and adoption of mobile Health (mHealth) apps to support healthcare research and clinical practice. mHealth apps have been widely adopted in chronic condition monitoring, remote patient monitoring, and disease treatment [1], testing, and data collection [2]. Prior research [3] has shown that combining mHealth apps with other interventions helps improve overall quality of care.

Security and privacy are key challenges that must be addressed when developing and deploying mobile technologies. In particular, sensitive patient data must be protected in mHealth apps, which may store users' eating habits [4], daily activities [5] or sleeping patterns [6]. This sensitive, private data may be collected by mobile devices (such as Android advertis-

ing networks[7] and passive collection mechanisms [8]) (such as connection between advertising identifiers and device-level identification). However, it can also intercepted and sold on the black market [9] and [10] since collected data can be linked with users' Google identities. Protecting the privacy of sensitive data requires rigorous authentication and security mechanisms, such as data-at-rest and data-in-transit encryption.

One element affecting mHealth app data-in-transit security is *Cyber-Physical Identity* (CPI) linkage, which connects a patient's digital identity in a medical record system (e.g., master patient identifier) to a physical mobile device. This linkage is vital to collect patient data accurately and securely. For example, a mismatched identity may cause incorrect information sent from a mobile device to enter the wrong patient record and impact treatment decisions, such as prescribing an incorrect dosage of opioids to the wrong patient.

The CPI linkage process is akin to checking arm bands in a hospital to ensure that the correct person is linked to a medical record. In the case of CPI linkage, however, patient records are linked to mobile device(s) that report health information related to that patient. The linkage process typically involves connecting a given credential with a patient's identity. For example, providers may either generate a long-term username/password recorded by a patient or provide a one-time security code on a billing statement.

To ensure security and identify validation, many authentication methods have complex workflows, which require users to follow a list of steps, such as providing email, phone number, and other identifiers. For mHealth apps, however, ensuring effective usability is essential since users are often (1) *patients with health problems*, who may be limited by mental or physical conditions or (2) *nurses and providers*, who have limited time and who already follow complex processes. Prior research shows that usability directly impacts the frequency of use and adoption of mHealth apps [11].

Privacy regulations also require data-at-rest be stored securely and meet certain requirements. For example, collected patient data must be stored in a *Health Insurance Portability and Accountability Act* (HIPAA)-compliant environment, which incurs higher cost and effort when developing mHealth apps, especially apps designed for small groups of healthcare providers. Online platforms (often created by healthcare research institutes) are one means for overcoming privacy challenges in data collection by providing secure data storage. For instance, Vanderbilt University created RED-Cap [12] in 2004 to support small groups of researchers collecting data in a HIPAA-compliant manner.

Key contributions. This paper extends our prior work [13] on evaluating mHealth authentication

techniques and examines an architectural pattern for adapting different mHealth authentication schemes to existing patient and research data information systems. In addition, this paper analyzes how various authentication and CPI establishment architectures impact the usability of mHealth apps for patients and providers.

For example, we explore a method for evaluating mHealth authentication method usability in the context of patient and provider burdens. In particular, we evaluate two popular 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—designed to overcome limitations with conventional approaches.

Paper organization. The remainder of this paper is organized as follows: Sec. 2. presents a case study, the PainCheck app, which is used throughout the paper to motivate the need for QR-Code token transfer and authentication; Sec. 3. summarizes different usability and process barriers that impede the adoption of mHealth apps and proposes evaluation methods to assess them; Sec. 4. describes the design of our QR-Code authentication architecture; Sec. 5. analyzes usability challenges in legacy authentication approaches and describes how our proposed authentication method uses QR codes and authentication tokens to address those challenges; Sec. 6. compares and contrasts our research with related work on mHealth security; and Sec. 7. presents concluding remarks and outlines future work.

2. Motivating Example

For decades, pain monitoring has played a critical role in healthcare [14] and [15]. Evidence extracted from published data [14] shows that concise postoperative pain measurement positively influences the pain management strategy. Researchers and clinicians attach great importance to subjective pain severity measurement [15], which helps determine appropriate dosage of pain medications.

This paper uses the PainCheck mHealth app as a case study to motivate our authentication and integration approaches. This app was developed at Vanderbilt University to help patients report their pain levels following thoracic surgery in both acute and post-acute settings. Figure 1 shows several screenshots of our PainCheck app.

Immediately following surgery, nurses, patients, and care-givers use PainCheck to report subjective pain levels for patients suffering from post-operative pain. Patients and care-givers can report pain scores in the hos-

pital and after leaving for a configurable period of time. With these timely pain reports, such as pain level and activity level, PainCheck can visualize patients' pain status, which helps providers quickly refine patients' pain management strategy. Unlike regular user-reported apps, patient data collected via PainCheck strictly follows healthcare privacy regulations.

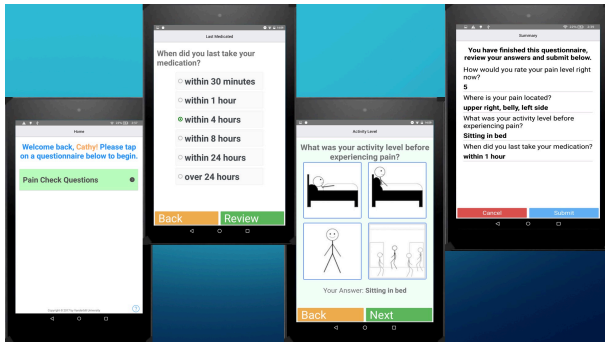


Fig. 1: Screenshots of the PainCheck App.

For example, the United States (US) requires healthcare data be stored in an HIPAA-compliant manner. We chose *Research Electronic Data Capture* (REDCap) [12] as the data management system to store data and design data collection instruments administered via mHealth apps. REDCap is a web app developed by Vanderbilt University that provides research teams with a reusable system to collect and manage clinical data and meet HIPAA and Institutional Review Board (IRB) standards for patient privacy.

REDCap is widely adopted in research communities and used in over 100 countries for over 612,000 projects, such as the Texas twin project [16], librarian-mediated literature searches [17], and biomedical research [18]. Integrating our PainCheck app with REDCap allowed us to leverage existing institutional knowledge on the use and operation of the system, as well as overcome challenges in deploying a resilient system that stores HIPAA-protected data securely.

Adherence to HIPAA privacy rules is required for US health research to protect data confidentiality [19]. However, researchers have observed that the HIPAA rules can negatively impact research progress in terms of cost and delays [20] and create compliance challenges in mHealth research for both providers and developers [21]. REDCap is designed to meet privacy requirements, which is an efficient resource for mHealth research to handle secure data storage without incurring the drawbacks of app-specific privacy considerations.

3. Usability Challenges in CPI-linkages of mHealth Apps

To help researchers understand how mHealth authentication methods impact patients and providers, this section examines several types of usability challenges incurred by different authentication approaches. This section also describes evaluation metrics we developed to measure how mHealth cyber-physical linkage and authentication approaches impact usability.

3.1. Memory Impediments

A "memory impediment" is a requirement for a patient to remember a specific set of information, such as a username/password or a process that must be followed. Remembering a long string of account/password characters can be hard for patients who are already in pain. Moreover, even healthy individuals rarely change their passwords and tend to use the same passwords among various services due to the effort needed to learn and remember new passwords.

A survey conducted by Telesign [22] revealed that 21 % and 47 % of people use 5-year old and 10-year old passwords, respectively. Moreover, 70 % of customers are concerned with their account security, but 73 % of accounts still use the same password. This practice is highly vulnerable to attack since hackers need only obtain access to one password to attack other accounts of the same owner. Password problems make up 20–30 % of all IT service desk volume [23], so requiring nurses or providers to manage credential transfer to patients can introduce a substantial usage barrier.

According to a survey conducted by HDI (339 service centers) [23], roughly 3 out of every 10 IT tickets received by support centers are related to password resets. To ensure security, 52 % of organizations require users to change their password every 3 months, and 28 % of them require higher frequency of password reset. Sixty-eight percent of organizations require customers to keep 2–5 passwords, while only 13 % need customers to remember just one password. For patients and providers, however, requiring changes in passwords can add a substantial burden. It is therefore beneficial to consider security approaches that maintain security without requiring patients and providers to continually learn new or complex credentials.

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. With the traditional username/password approach, users must remember an amount of data proportional to the length of the credential pair (i.e., it is $O(N)$, where N is length of characters users need to remember). Longer passwords tend to increase security by protecting user account information against attacks, so providers may add a layer of protection that requires users to create a password with a minimum length, which creates extra work for users to remember a longer password.

In contrast, encrypted credentials provided by some authentication methods alleviate users from remembering complicated credentials. These methods map user information with an arbitrarily long token. The length of this token has no effect on how much the user must remember (i.e., it is $O(1)$, where the character users need to remember is not related to token length).

M2. The duration that patients need to remember the data relative to length of treatment. The duration that patients need to remember their credentials is flexible for mHealth apps. Target user groups of mHealth apps vary depending on the functions offered by a certain app. For our PainCheck app, the majority of target users could be chronically ill patients suffering from pain, patients who have undergone a surgery, or those who are recovering from a surgery and are under observation. In these cases, users must only remember their credential data for a certain period of time, e.g., as long as they are active users of the app. Conversely, the frequency and duration of using in-hospital mHealth app could be decided by providers. When the frequency is low and the duration is short, the likelihood of users forgetting their password increases.

We use metrics M1 and M2 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 there are in the underlying security credential used to authenticate, such as $O(N)$ characters, where N is the length of the security credential.

As shown in Sec. 5, other authentication approaches just require the patient to remember a specific password, which only has a one-time use. This password can then be exchanged by the device for an authentication token that can be much more complex than the original password. The authentication credential and the password are therefore decoupled because 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 in this approach is $O(1)$ since the length of the one-time password is constant and independent of the length

of the 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.

3.2. Physical Impediments

Physical impediments are operations a patient must perform during the authentication process, including pressing on a mobile device, typing on the device, or shaking the device. According to a survey in 2003 [24], 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 device virtual keyboards compared to typing on a physical keyboard. Likewise, 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 should minimize these physical impediments to facilitate use. We hypothesized that an ideal authentication method should reduce these impediments to improve user experience while maintaining equivalent security. To evaluate this hypothesis, we analyzed total characters typed relative to credential length and total characters typed for credential recovery relative to credential initialization. We therefore propose the following two measures of physical impediments to assess mHealth authentication approaches:

Ph1. Total characters typed relative to credential length. For username/password authentication, the amount of characters patients need to type is linearly dependent on the length of credential pairs (i.e., it is $O(N)$, which is equal to the length they need to remember). If credentials are encrypted by an authentication method, patients only need to input constant characters (i.e., it is $O(1)$).

Ph2. Total characters typed for credential recovery relative to credential initialization. When patients lose or forget their credentials, they must update their credentials via a credential recovery mechanism, which may require patients to provide additional identity information (such as a phone number or email address) to retrieve credentials securely.

For example, a password reset link will be sent to the corresponding email address so that patients can create new passwords. In this case, the total of characters typed is same as credential initialization (i.e., it is $O(N)$). For some authentication methods, both credential initialization and credential recovery process require no data input (i.e., it is $O(1)$).

Similar to the memory impediments, we measure physical impediments in terms of how much typ-

ing 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 independently of how much data a patient enters.

3.3. 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. To help patients master an app quickly, medical staff can provide detailed instructions, such as helping patients create accounts and bind identities to accounts. However, nurses (who often play the role of an instructor) perform many other tasks during their shift. To reduce the workload of medical staff, therefore, authentication methods should be simplified by minimizing the total process steps required of providers.

P2. Total process steps for patients. When starting to use an mHealth app, patients using mobile devices must be authenticated by following certain steps, such as receiving short messages, typing on device and getting access authorizations. Patients recovering from surgical procedures are usually fatigued, however, which makes it impractical for them to concentrate on complex or long instructions. Thus, mHealth apps should consider reducing as many process steps as possible.

P3. Total error-prone steps. Complexity exists in different steps for both patients and providers, which makes some steps more error-prone than others. For example, mistakes tend to happen in steps related to typing operations. Error-prone steps bring higher barriers for users since more concentration is required of patients and providers to avoid potential mistakes.

P4. Revocation steps at the end of treatment. Revoking each patient's access manually poses a higher requirement from providers (i.e., they must remember every patient's credential status) and is also error-prone (e.g., the wrong patient's access may be revoked). By providing a revocation mechanism during authentication process, patients' access to apps can be auto-revoked at the end of treatment, thereby lightening the process burden for providers.

3.4. Other Impediments

Other impediments incur additional demands, such as cost and hardware usage, that are unique to a specific approach. When adopting an authentication method, providers may need to pay for other resources besides basic computing resources, including third-party service fee or hardware fee. For example, the SMS authentication systems require a mobile device to have cellular service, as well as a network connection, whereas other approaches do not require cellular service.

For example, a static username/password is vulnerable for services that involve sensitive data, such as financial or banking services. To overcome this problem, smart cards [25] can be used to generate dynamic passwords. Smart cards can create a *One-Time Password* (OTP) for bank systems and provide core *Public Key Infrastructure* (PKI) services [25] and [26]. However, using extra hardware (such as smart cards) can impede adoption of an authentication method due to implementation costs and the need to carry them in person. We measure other barriers in terms of additional costs for providers and addition requests for patients.

4. Integrating Alternative Authentication Mechanisms with Legacy Health Systems

CPI-linkage and authentication alternatives offer different advantages, such as reduced patient/provider burden. In practice, however, it may not be possible to employ a given approach due to design decisions "hard-coded" into legacy patient data management systems.

For example, many existing systems for capturing medical data are designed with the assumption that trusted medical providers will input the data on behalf of patients. As discussed in Sec. 5.1. and Sec. 5.2. , however, patient-reported outcomes require direct reporting of data from patients. This difference in design stemming from who is expected to enter data creates an architectural mismatch that must be overcome to realize more effective authentication schemes for mobile devices. To realize the benefits of alternative CPI-linkage and authentication approaches, architectural patterns [27] can be applied to resolve this conflict.

In most existing medical records systems, staff and providers perform the step of CPI-linkage by asking the patient for identifying information, such as their name, date of birth, and phone number, and then looking up the corresponding cyber-identity of the physical person in front of them in the medical records sys-

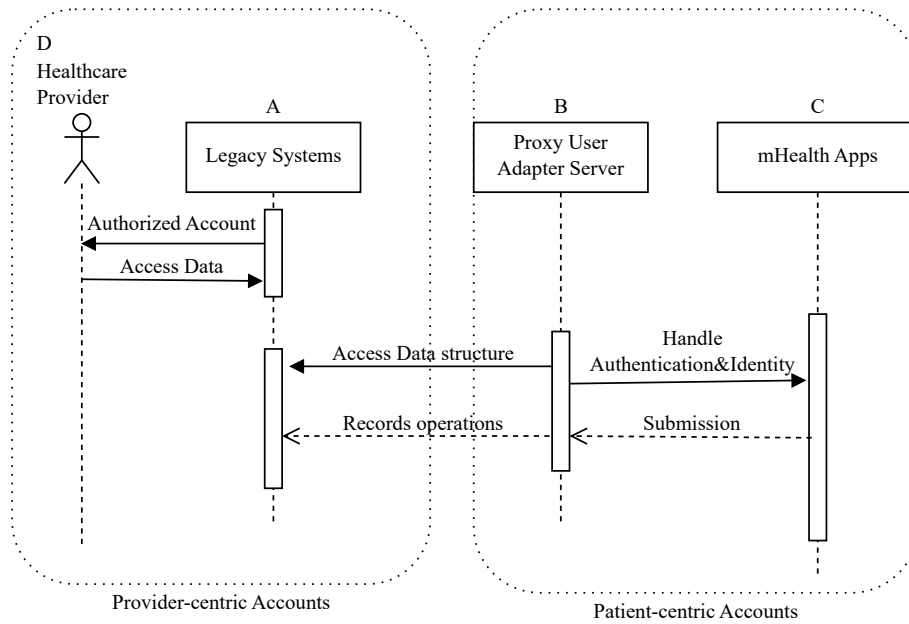


Fig. 2: The Structure of a Proxy Server.

tem. After this linkage step is performed, the staff or provider directly enters data about the patient into the system since the patient does not directly enter their data into the medical records system or have an account. For mHealth apps, however, the CPI linkage must be performed to link patient mobile devices to their records and then access must be delegated to the devices so patients can directly enter data about themselves (e.g., patient-reported outcomes).

The remainder of this section explores an architectural pattern, called *Proxy User Adapter*, that can be applied to integrate mHealth apps with QR-codes [28], which are two-dimensional barcodes providing fast readability and compact storage capacity. QR-codes can be used to link patient devices securely with their corresponding records in systems designed for data entry by trusted users. Moreover, this pattern enables direct insertion of data from a patient into the system without changing the existing architecture of these systems from a model based on data entry by trusted users. The *Proxy User Adapter* pattern enhances the *Proxy* pattern [29] to provide an authentication proxy in context of legacy hospital systems.

4.1. REDCap Integration Case Study

To motivate the challenges of integrating a QR-code authentication scheme into legacy data management systems, we discuss our experience integrating the PainCheck app based on QR-Code authentication with legacy research data management systems for patients at the Vanderbilt University Medical Cen-

ter (VUMC). We initially considered creating our own stand-alone data management system specifically for mHealth data. However, the complexities of providing high-assurance secure data storage in HIPAA-Compliant environment made starting from scratch impractical. Moreover, training is a major consideration since our goal is to support healthcare providers who have limited time to learn new systems and incorporate them into their research and clinical workflows.

The architecture of the PainCheck app is shown in Fig. 2. REDCap is shown in Item A and is responsible for data storage and designing metadata, which defines the basic attributes of a project/questionnaire, such as the number or type of questions. The mHealth app, shown in Item C, is responsible for displaying data collection instruments, such as pain checks, to patients. The proxy user adapter, shown in Item B, is responsible for adapting the mobile device-centric authentication and security model of the mobile app to the trusted user architecture of existing legacy patient data management systems.

Even though healthcare providers can generate a form in REDCap to collect patients’ identities, linking identities by filling out a form is not a secure CPI-linkage method, as we discuss in Sec. 1. . Since mistakes can be made when manually entering data for CPI-linkage, these identities may be inaccurate and affect either treatment decisions or the accuracy of collected clinical data. Thus, although REDCap does support form-based entry of patients by data on the web, it is designed primarily for trusted users.

To overcome the issue with trusted users, we introduce a proxy user adapter, which plays the role of con-

necting patients and providers with the REDCap system, which is a HIPAA-compliant platform shown in Fig. 3. REDCap has been widely adopted by developers and providers at VUMC and other healthcare systems. REDCap also provides mobile collection facilities, such as the REDCap Mobile App [12].

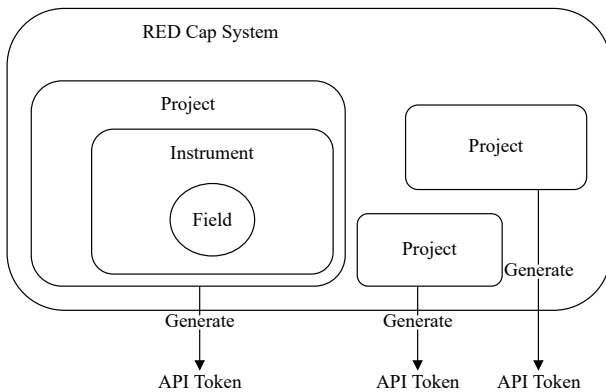


Fig. 3: Diagram of REDCap Structure.

At VUMC medical records and clinical research data are processed by Epic and REDCap respectively. Clinical data, such as lab results and provider notes, are stored in Epic. Due to legal considerations, storage of patient-reported research data, such as pain and activity levels, are stored separately from Epic in REDCap.

To submit new reports in a REDCap project, trusted users need an API token, which is generated in the REDCap web app and bound to a REDCap account. Project data can be exported and modified by external tools, whose actions are limited by the user account rights associated with the API token. As mentioned in Sec. 3, however, a patient-created account might not match the desired CPI-linkage and authentication model whereby devices are bound to patient records, increasing patient burden (and thus resistance) to use an app. It is hard to implement our QR-Code Authentication schema with these user-centric authentication systems that were not built to integrate mobile devices in their authentication model.

Based on our experiences, we identified the following challenges of integrating QR-code-based authentication with these types of systems:

- **Trusted user-based authorization system.** Since accessing these systems requires tokens generated by authorized accounts in the web browser, patients do not have permission to input data to the system without an account. However, the servers in the QR-code-based authentication approach from Sec. 5.2 need to assign each patient a unique access token for authorization and CPI linkage, which may not be supported.

- **Limited ability to customize authentication structure in legacy applications.** Researchers often cannot customize the structure of the application authentication architecture, such as REDCap's API token authentication or data format. It is therefore necessary to build an integrated design pattern to implement alternative authentication schemes to integrate with legacy applications.

4.2. The Proxy User Adapter Pattern

The *Proxy User Adapter* architectural pattern (shown in Fig. 2) consists of middleware that bridges the various CPI-linkage and authentication models of mHealth apps and the underlying trusted-user-focused patient data system, such as REDCap. This pattern employs identity-based tokens to authenticate patients when interacting with mHealth apps. Likewise, the proxy user adapter component holds a credential of one or more trusted users in the target patient data system that it uses to store data on behalf of the mobile devices. By applying this pattern, a facility for adapting the authentication model of the mHealth device to that of the patient data system is enabled by proxy-ing data submissions through one or more trusted user accounts in the patient data storage system.

In our implementation of the PainCheck app on REDCap, the *Proxy User Adapter* pattern is employed to separate the functionality of secure data storage and patient authentication. This pattern employs an API token, which is authentication key that provides programmatic access to a trusted user's account in REDCap, and uses the token to access and operate upon data in REDCap. Each request from a mobile device is proxied through a trusted REDCap user's account that is associated with the API token.

PainCheck's QR-code-based authentication (described in Sec. 5.2) is implemented at the proxy user adapter rather than being built into REDCap. This approach enables patients to access mHealth apps on their mobile devices and join research studies by scanning QR-codes with access tokens. The *Proxy User Adapter* pattern is therefore a conduit for passing requests to REDCap and does not store any patient data that transits through it.

As shown in Fig. 2, after creating a data collection instrument (which is a form for collecting patient data) in REDCap's online designer, healthcare providers register their API tokens with the proxy user adapter. This adapter imports the instrument and proxies the submission of data from mobile devices. Authorization interactions between the proxy user adapter and app clients follow the rules covered in Sec. 5.2.

Trade-offs When Applying the Proxy User Adapter Pattern. The *Proxy User Adapter* pattern decouples mHealth apps from the authentication and CPI-linkage approach of the underlying patient data management system. At the same time, however, this pattern introduces the following security considerations that must be made explicit:

- The proxy user adapter requires the intermediate proxy server to hold credentials belonging to a trusted account, which in turn requires credentials to be protected properly and only possess the minimum privileges needed to proxy the required requests on behalf of mHealth apps. In particular, where possible, credentials should allow write-only access and no facility to read and extract data. For patient data systems that support OAuth 2.0, the proxy server can hold an OAuth token that is generated for it and scoped to the appropriate permissions for requests it needs to proxy.
- Since all patient-reported outcomes transit through the proxy user adapter, the proxy server must not store confidential data inadvertently. Developers must ensure that common practices, such as logging of requests, do not accidentally capture and store patient data. Proper application of the proxy server requires a careful security audit to ensure that requests are simply forwarded on to the backing patient data management system.
- Any request buffering or queuing/retry behavior must be implemented at the mHealth client. Since the proxy server should not capture or store patient data, transient errors due to network issues, patient data management system outages, or other unexpected events must be managed at the mHealth app. While it is tempting to allow the proxy to handle buffering and retry logic on behalf of the mHealth app, this approach introduces security risks in the proxy that are better handled at the client since it should have retry logic to handle connection issues to the proxy server.

Benefits of the Proxy User Adapter Pattern. The *Proxy User Adapter* pattern provides researchers and clinicians with an efficient way for mHealth apps to adopt the most appropriate authentication mechanism without modifying existing information systems. Legacy systems are usually designed for trusted users to manage medical data and clinical systems that patients are not authorized to access directly. For example, REDCap adopts provider-centric accounts, requiring providers to collect data from patients, rather than offering a patient-centric account. A solution is

to add new patient-centric account mechanisms to supply patient-reports apps in REDCap.

In practice, however, integrating existing systems with various mHealth apps by appending a new authentication approach is hard for developers. In particular, developers must fully understand the structure of legacy systems to add new parts carefully without disrupting existing functionality. Moreover, systems developed by third-parties (such as VUMC's use of Epic) may not allow direct modification of the authentication architecture onsite. Adopting the *Proxy User Adapter* pattern thus provides developers with greater flexibility to customize their authorization server.

5. Evaluating Authentication Methods

This section describes how we apply QR-Code-based authentication to substitute legacy authentication methods (username and password authentication) according to our discussion in Sec. 4. . Section 5.1.

evaluates a common legacy authentication method (username and password authentication), which incurs significant impediments and burden on patients and providers. To overcome potential shortages of legacy authentication systems, Sec. 5.2. describes how we applied QR-Codes and authentication tokens to improve usability for our PainCheck app developed based on REDCap.

5.1. Username/password

Username/password authentication is widely used in legacy healthcare systems. 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 perform operations on the data in that account, such as sending pain information to the server.

When username/password authentication is implemented in the PainCheck app, patients can use any device to input pain data as long as they enter a valid username/password on that device. After verification, the new hashed password will replace the previous one in the table. These credentials will not expire.

With username/password-based systems, credential and identity establishment is relatively independent. The system cannot recognize authorized users if users do not enter their identity/profile manually. To avoid falsified or incorrect identities, additional workflow is

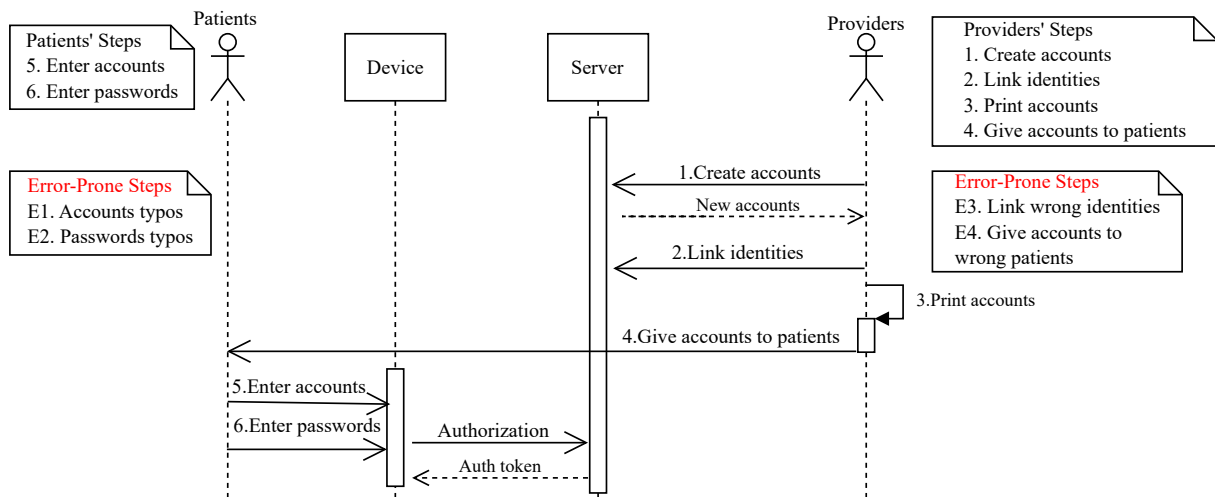


Fig. 4: Diagram of Username/Password Authentication.

required for CPI linkage in this structure. The server needs to pre-validate the identity entered by patients.

Credential transfer to users. Only patients who are actively receiving treatment should submit pain data to the PainCheck app, thereby prevent invalid data from arbitrary users. Providers thus need to control account creation and physical identity establishment. To link a new device to a patient’s PainCheck account, a provider must create a username/password for the patient and/or coordinate the collection of username/password from the patient to create the account.

Electronic Medical Record (EMR) systems can also help providers auto-generate a pair of username/temporary password for patients the first time they access an EMR system. Patients need to create their new passwords after entering an application. In either case, a coordination step must occur to collect or distribute a username/password to/from a patient, as shown in steps 1–4 of Fig. 4.

Table 1 applies the metrics from Sec. 3. 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 need to remember the data is the length of the treatment period, which is also $O(N)$.

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 1 shows the evaluation of metrics P1–P3 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. Likely errors incurred during the 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) incorrect usernames/passwords being entered 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. Initial passwords are normally generated randomly (which may include letters, numbers, or special characters). It will therefore 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 if a random password is generated for the patient since human-produced passwords are prone to dictionary (and other) attacks [30]. 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 Tab. 1.

Re-linkage of Devices to Different Patient Accounts. The shared in-hospital device can be used either by patients or nurses, so switching accounts on same device happens regularly. Anyone can access the shared device. Therefore, an administrator account (which can input data for any patient) is not an optimal solution due to the potential invalid data entered by a wrong person. Patients have to re-enter credential pairs every time when they need to switch accounts.

Tab. 1: Evaluation of Authentication Methods.

	Metrics	Username/password	QR+OTP
M1	Total characters remembered relative to credential length	$O(n)$	$O(1)$
M2	The duration that patients need to remember the data relative to length of treatment	$O(n)$	$O(1)$
Ph1	Total characters typed relative to credential length	$O(n)$	$O(1)$
Ph2	Total characters typed for credential recovery relative to credential initialization	$O(n)$	$O(1)$
P1	Total process steps for provider	4	1
P2	Total process steps for patient	2	1
P3	Total error-prone steps	4	1
P4	Revocation Steps at the end of treatment	2	0
	Binary Metrics		
O1	Additional costs / Barriers	NO	NO

Credential Loss & Recovery. In the event that a patient or caregiver forgets their username/password, a credential recovery process must be followed. For example, a provider may need to 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 Tab. 1.

Credential Revocation at the End of Treatment. At the end of the treatment period, providers can manually delete patients' accounts to revoke their permissions. Nurses need to check the status of patients before they leave hospitals and revoke their credentials in a database, so there are two revocation steps at the end of treatment, as shown in metric P4 in Tab. 1. If patients come to the same hospital in the future, they will be assigned new accounts.

5.2. Integrating Legacy System with QR-Code-based Authentication

To overcome the limitations described in Sec. 3, we designed an alternative authentication approach that combines OTPs with transfer via QR-Codes. With this approach, OTPs are generated for each device, as shown in Fig. 5.

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. It also eliminates the requirement for a cellular connection and the risk that the OTP is sent to the wrong device accidentally.

Only devices physically near the provider can possibly receive the OTP by scanning the provider's mobile device or printed sheet of paper. Providers should protect patients' QR-Codes carefully, however, to prevent malicious usage from third-parties. For example, cameras with high resolution can scan QR-Codes from distant locations.

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 the loss (e.g., it can become invalid three hours after generation).

5.3. Key Processes in QR-Code-based Authentication

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 needs not to remember any credentials at all, as shown in Tab. 1.

CPI Linkage of Mobile Devices. Table 1 shows the evaluation of metrics P1–P3 for this linkage process. Providers must only choose the correct patient to generate the QR-code for, as shown in Step 1 of Fig. 5. Likewise, patients must only scan the QR-code, as shown in Step 2. The main errors that can occur are selecting the wrong patient to generate a QR-code for or showing the wrong QR-code to the patient.

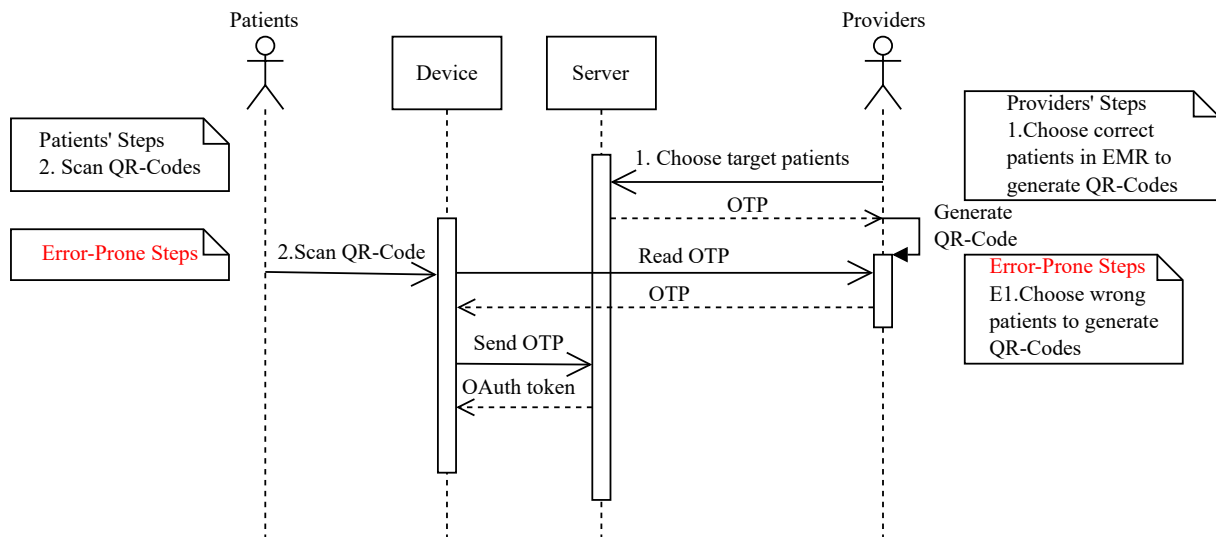


Fig. 5: Diagram of QR-Code-based Authentication.

Credential Entry on Devices. Credential transfer is automated and the total characters typed relative to credential length is $O(1)$, as shown in metric Ph1.

Credential Loss & Recovery. Credentials are automatically remembered by the mHealth app and credential loss is not possible.

Re-linkage of Devices to Different Patient Accounts. If QR-based authentication is adopted for an in-hospital device, nurses must switch between accounts by scanning a new QR-code. For patients or caregivers using an in-hospital device, a nurse’s help is required to authenticate their account on this device.

Credential Revocation at the End of Treatment. Providers can decide the length of patient credentials in every treatment. No revocation steps are needed at the end of treatment, as shown in metric P4 in Tab. 1.

6. Related Work

This section summarizes the differences between our research and related work on mHealth security and usability. Most prior work does not discuss the interplay between mHealth security and patient/provider burden. We explore relevant prior work in each of these areas separately.

We cover related work by presenting (1) an overview of prior work on mHealth authentication approaches, (2) analyzing related metrics for mHealth app usability, and (3) discussing different strategies to integrate healthcare legacy system in different scenarios.

6.1. Authentication in mHealth Apps

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 [31] and [32]. Attacks from the outside, however, are not the only threat that must be handled for mHealth apps. In particular, Kotz et al. have categorized privacy-related threats in mHealth systems [33], which can be posed by not only malicious third parties but also service providers and patients (inside threats). For example, patients themselves could share their credentials with others and expose their private data.

The impact of security on usability [11] is not widely studied by mHealth authentication researchers. Our paper complements existing authentication literature by defining metrics for analyzing burden that authentication processes place on patients and providers and shows how different authentication processes lessen these burden without compromising security. Moreover, our paper provides an architectural pattern (*Proxy User Adapter* described in Sec. 4.) for integrating newer authentication approaches with legacy patient data management systems that lack support for these alternate authentication formats.

6.2. Mobile App Usability

Significant prior research addresses ways to improve mobile app usability and overcome mobile device limitations, such as the small screen sizes and touch-based displays [34], [35] and [36]. To assess mobile app usability, researchers have proposed various eval-

uation methodologies, such as laboratory experiments and field studies [34] and [37]. The evaluation methodologies are primarily qualitative metrics based on user preference or assessments through A/B testing that assess how differing designs affect a goal metric, such as menu completeness of a mobile wireless information system [37].

A challenge in evaluating mobile app usability is defining standardized objective measurements of usability. To ensure accurate measurement, previous research often combines both objective and subjective metrics. For example, the ISO 25062/ISO 9241 and QUIS 7.0 standard questionnaires are used to measure mobile app usability of the Google Maps [38]. An alternative strategy is to analyze usability aspects of mobile apps by modeling approaches [39]. Other researchers have looked at usability issues of username/password authentication on mobile devices by collecting data on users' input time and failure frequency [40].

The evaluation methods presented in Sec. 3. complement existing usability metrics and provide quantitative measures of cognitive, physical, and process burdens specific to healthcare. These specific burdens are not assessed in a healthcare context in prior work, but are critical to understand and assess the design of mHealth technologies. For example, a design that scores high on usability for patients may place an undue burden on provider workflows and thus be undesirable when analyzed in the overall healthcare context.

6.3. Integration Strategies with Legacy Patient Data Management Systems

Hospital information systems are responsible for managing both medical records and research data and are usually built with a focus on input of data from staff or other trusted users, who are typically *not* patients. With the rapid development of mobile technologies and demands for data capture outside of the clinical setting, such as increasing number of mHealth apps, it has become a challenge to integrate existing systems with a patient-centric data capture model. Some research has investigated new service architectures and frameworks to integrate edge technology with legacy information systems [41] and [42].

For example, Li-Fan et al. propose a middleware framework to transit data from legacy information system to a more robust and scalable system in the National Taiwan University Hospital [41] so that heterogeneous information systems can be integrated with existing medical record data. Researchers have also discussed interactive strategies to integrate with healthcare legacy system in different scenarios [43], [44] and [45], such as wireless web-enabled devices, exter-

nal systems accessing medical records and home health services.

In this paper, the *Proxy User Adapter* architectural pattern presented in Sec. 4. complements prior work on integration by providing a standard architectural model to connect legacy medical record systems with alternative authentication and CPI-linkage mechanisms that are better suited for mHealth apps.

7. Concluding Remarks

This paper discussed usability challenges that arise when integrating new mHealth apps with legacy data storage systems by evaluating a set of mHealth authentication techniques to determine (1) how they impact clinical workflows and (2) what types of impediments they place on patients and providers. We also presented several metrics for quantifying the identified impediments, including the amount of information that patients must remember and the number of steps that are added to a clinical workflow.

The results of our analyses showed that different authentication techniques have steps of roughly the same complexity, though a wide variation exists across authentication approaches in terms of the total number of steps, amount of information that patients must remember, and types of errors. Conversely, the proxy user adapter allows developers to apply new authentication approaches that have higher usability, without modifying legacy system authentication processes.

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 common, but not ideal, for mHealth apps in acute care settings. Barriers in Sec. 3. explore potential usage problems encountered by patients.
- The QR-code + OTP method described in Sec. 5. preserves the key usability improvements of conventional authentication techniques, but eliminates the requirement for cellular service and the potential of sending credentials to the wrong person.

Our future work focuses on extending our research to outpatients so that mHealth apps like PainCheck can provide patients with highly-usable authentication methods, even if they do not reside in a hospital setting. We also realize there are other ways to evaluate authentication methods in mHealth apps besides our metrics, which focus largely on usability for patients

and providers. We are therefore improving and extending our evaluation methods to provide more adequate and complete metrics.

Acknowledgment

This paper was supported in part by National Science Foundation Award# 1552836.

Author Contributions

Z.T. and X.L. carried out the experiment. Z.T. wrote the manuscript with support from P. Z., W.N., D.G., D.C.S., M.C., and J.W. J.W., D.C.S., J.C.N., M.C., and D.G. supervised and led the experimental design of the project.

References

- [1] LEACH-LEMENS, C., J. A. BLAYA and H. S. FRASER. Using mobile phones in HIV care and prevention. *HIV & AIDS Treatment in Practice*. 2009, vol. 137, iss. 7.
- [2] FREE, C., G. PHILLIPS, L. FELIX, L. GALLI, V. PATEL and P. EDWARDS. The effectiveness of M-health technologies for improving health and health services: a systematic review protocol. *BMC Research Notes*. 2010, vol. 3, iss. 1, pp. 1–7. ISSN 1756-0500. DOI: 10.1186/1756-0500-3-250.
- [3] LABRIQUE, A. B., L. VASUDEVAN, E. KOCHI, R. FABRICANT and G. MEHL. mHealth innovations as health system strengthening tools: 12 common applications and a visual framework. *Global Health: Science and Practice*. 2013, vol. 1, iss. 2, pp. 160–171. ISSN 2169-575X. DOI: 10.9745/GHSP-D-13-00031.
- [4] GILL, S. and S. PANDA. A Smartphone App Reveals Erratic Diurnal Eating Patterns in Humans that Can Be Modulated for Health Benefits. *Cell Metabolism*. 2015, vol. 22, iss. 5, pp. 789–798. ISSN 1550-4131. DOI: 10.1016/j.cmet.2015.09.005.
- [5] TURNER-MCGRIEVY, G. M., M. W. BEETS, J. B. MOORE, A. T. KACZYNSKI, D. J. BARR-ANDERSON and D. F. TATE. Comparison of traditional versus mobile app self-monitoring of physical activity and dietary intake among overweight adults participating in an mHealth weight loss program. *Journal of the American Medical Informatics Association*. 2013, vol. 20, iss. 3, pp. 513–518. ISSN 1527-974X. DOI: 10.1136/amiajnl-2012-001510.
- [6] CHAUDHRY, B. M. Sleeping with an Android. *mHealth*. 2017, vol. 3, iss. 2, pp. 1–2. ISSN 2306-9740. DOI: 10.21037/mhealth.2017.02.04.
- [7] DEMETRIOU, S., W. MERRILL, W. YANG, A. ZHANG and C. A. GUNTER. Free for All! Assessing User Data Exposure to Advertising Libraries on Android. In: *Network and Distributed System Security Symposium (NDSS)*. San Diego: Internet Society, 2016, pp. 1–15. ISBN 978-1-891562-41-9. DOI: 10.14722/ndss.2016.23082.
- [8] SCHMIDT, D. C. Google data collection research. In: *Digital Content Next* [online]. 2018. Available at: <https://digitalcontentnext.org/blog/2018/08/21/google-data-collection-research/>.
- [9] GORDON, W. J., A. FAIRHALL and A. LANDMAN. Threats to Information Security—Public Health Implications. *The New England Journal of Medicine*. 2017, vol. 377, iss. 8, pp. 707–709. ISSN 1533-4406. DOI: 10.1056/NEJMp1707212.
- [10] LIU, V., M. A. MUSEN and T. CHOU. Data Breaches of Protected Health Information in the United States. *Jama*. 2015, vol. 313, iss. 14, pp. 1471–1473. ISSN 0098-7484. DOI: 10.1001/jama.2015.2252.
- [11] GAGNON, M.-P. A Systematic Review of Factors Associated to M-Health Adoption by Health Care Professionals. In: *Medicine 2.0 Conference*. Malaga: Journal of Medical Internet Research (JMIR) Publications Inc., 2014.
- [12] HARRIS, P. A., R. TAYLOR, R. THIELKE, J. PAYNE, N. GONZALEZ and J. G. CONDE. Research electronic data capture (REDCap)—a metadata-driven methodology and workflow process for providing translational research informatics support. *Journal of Biomedical Informatics*. 2009, vol. 42, iss. 2, pp. 377–381. ISSN 1532-0464. DOI: 10.1016/j.jbi.2008.08.010.
- [13] TENG, Z., P. ZHANG, X. LI, W. NOCK, M. RODRIGUEZ-CANCIO, J. WHITE, D. C. SCHMIDT, D. GILMORE and J. C. NESBITT. Authentication and Usability in mHealth Apps. In: *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*. Ostrava: IEEE, 2018, pp. 1–6. ISBN 978-1-5386-4294-8. DOI: 10.1109/HealthCom.2018.8531158.

- [14] DOLIN, S. J., J. N. CASHMAN and J. M. BLAND. Effectiveness of acute postoperative pain management: I. Evidence from published data. *British Journal of Anaesthesia*. 2002, vol. 89, iss. 3, pp. 409–423. ISSN 0007-0912. DOI: 10.1093/bja/89.3.409.
- [15] JENSEN, M. P., P. KAROLY and S. BRAVER. The measurement of clinical pain intensity: a comparison of six methods. *Pain*. 1986, vol. 27, iss. 1, pp. 117–126. ISSN 0304-3959. DOI: 10.1016/0304-3959(86)90228-9.
- [16] HARDEN, K. P., E. M. TUCKER-DROB and J. L. TACKETT. The Texas Twin Project. *Twin Research and Human Genetics*. 2013, vol. 16, iss. 1, pp. 385–390. ISSN 1839-2628. DOI: 10.1017/thg.2012.97.
- [17] LYON, J. A., R. GARCIA-MILIAN, H. F. NORTON and M. R. TENNANT. The Use of Research Electronic Data Capture (REDCap) Software to Create a Database of Librarian-Mediated Literature Searches. *Medical Reference Services Quarterly*. 2014, vol. 33, iss. 3, pp. 241–252. ISSN 1540-9597. DOI: 10.1080/02763869.2014.925379.
- [18] KLIPIN, M., I. MARE, S. HAZELHURST and B. KRAMER. The Process of Installing REDCap, a Web Based Database Supporting Biomedical Research: The First Year. *Applied Clinical Informatics*. 2014, vol. 5, iss. 4, pp. 916–929. ISSN 1869-0327. DOI: 10.4338/ACI-2014-06-CR-0054.
- [19] ANNAS, G. J. HIPAA Regulations — A New Era of Medical-Record Privacy? *The New England Journal of Medicine*. 2003, vol. 348, iss. 15, pp. 1486–1490. ISSN 1533-4406. DOI: 10.1056/NEJMLim035027.
- [20] NESS, R. B. Influence of the HIPAA Privacy Rule on Health Research. *Jama*. 2007, vol. 298, iss. 18, pp. 2164–2170. ISSN 0098-7484. DOI: 10.1001/jama.298.18.2164.
- [21] LISS, B. HIPAA and Mobile Health. *New Jersey Lawyer*. 2016, vol. 21, iss. 1, pp. 20–24. ISSN: 0195-0983.
- [22] TeleSign Consumer Account Security Report. In: *TeleSign* [online]. 2015. Available at: <https://www.telesign.com/search?query=Telesign+consumer+account+security+report>.
- [23] Password-Reset Practices in Support. In: *ThinkHDI* [online]. 2012. Available at: <https://www.thinkhdi.com/library/supportworld/2011/password-reset-practices>.
- [24] RUSSO, C. A. and A. ELIXHAUSER. Healthcare Cost and Utilization Project (HCUP) Statistical Briefs: Hospitalizations in the elderly population, 2003 [online]. Rockville: Agency for Healthcare Research and Quality, 2006.
- [25] CHIEN, H.-Y., J.-K. JAN and Y.-M. TSENG. An Efficient and Practical Solution to Remote Authentication: Smart Card. *Computers & Security*. 2002, vol. 21, iss. 4, pp. 372–375. ISSN 0167-4048. DOI: 10.1016/S0167-4048(02)00415-7.
- [26] SANDBERG, L. and K. RODBERG-LARSEN. US7024226B2. *Method for enabling PKI functions in a smart card*. Washington, DC: U.S. Patent and Trademark Office, 2006.
- [27] BUSCHMANN, F., K. HENNEY and D. C. SCHMIDT. *Pattern-Oriented Software Architecture: A Pattern Language for Distributed Computing*. 4th. ed. New York: John Wiley & Sons, 2007. ISBN 978-0-470-05902-9.
- [28] ROUILLARD, J. Contextual QR Codes. In: *2008 The Third International Multi-Conference on Computing in the Global Information Technology (iccg 2008)*. Athens: IEEE, 2008, pp. 50–55. ISBN 978-0-7695-3275-2. DOI: 10.1109/IC-CGI.2008.25.
- [29] HANNEMANN, J. and G. KICZALES. Design pattern implementation in Java and aspectJ. In: *Proceedings of the 17th ACM SIGPLAN conference on Object-oriented programming, systems, languages, and applications (OOPSLA)*. Seattle: ACM Press, 2002, pp. 161–173. ISBN 978-1-58113-471-1. DOI: 10.1145/582419.582436.
- [30] PINKAS, B. and T. SANDER. Securing passwords against dictionary attacks. In: *Proceedings of the 9th ACM Conference on Computer and Communications Security*. Washington: ACM Press, 2002, pp. 161–170. ISBN 978-1-58113-612-8. DOI: 10.1145/586110.586133.
- [31] LEE, C.-I. and H.-Y. CHIEN. An Elliptic Curve Cryptography-Based RFID Authentication Securing E-Health System. *International Journal of Distributed Sensor Networks*. 2015, vol. 11, iss. 12, pp. 1–7. ISSN 1550-1477. DOI: 10.1155/2015/642425.
- [32] JIANG, Q., X. LIAN, C. YANG, J. MA, Y. TIAN and Y. YANG. A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth. *Journal of Medical Systems*. 2016, vol. 40, iss. 11, pp. 1–10. ISSN 1573-689X. DOI: 10.1007/s10916-016-0587-1.
- [33] KOTZ, D. A threat taxonomy for mHealth privacy. In: *2011 Third International Conference on*

- Communication Systems and Networks (COM-SNETS 2011)*. Bangalore: IEEE, 2011, pp. 1–6. ISBN 978-1-4244-8953-4. DOI: 10.1109/COM-SNETS.2011.5716518.
- [34] NAYEBI, F., J.-M. DESHARNAIS and A. ABRAN. The state of the art of mobile application usability evaluation. In: *2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*. Montreal: IEEE, 2012, pp. 1–4. ISSN 978-1-4673-1433-6. DOI: 10.1109/CCECE.2012.6334930.
- [35] COURSARIS, C. K. and D. J. KIM. A Meta-Analytical Review of Empirical Mobile Usability Studies. *Journal of Usability Studies*. 2011, vol. 6, iss. 3, pp. 117–171. ISSN 1931-3357.
- [36] LEE, D., J. MOON, Y. J. KIM and M. Y. YI. Antecedents and consequences of mobile phone usability: Linking simplicity and interactivity to satisfaction, trust, and brand loyalty. *Information & Management*. 2015, vol. 52, iss. 3, pp. 295–304. ISSN 0378-7206. DOI: 10.1016/j.im.2014.12.001.
- [37] GAFNI, R. Usability Issues in Mobile-Wireless Information Systems. *Issues in Informing Science & Information Technology*. 2009, vol. 6, iss. 1, pp. 755–769. ISSN 1547-5867. DOI: 10.28945/1095.
- [38] MOUMANE, K., A. IDRI and A. ABRAN. Usability evaluation of mobile applications using ISO 9241 and ISO 25062 standards. *SpringerPlus*. 2016, vol. 5, iss. 1, pp. 1–15. ISSN 2193-1801. DOI: 10.1186/s40064-016-2171-z.
- [39] GOEL, S., R. NAGPAL and D. MEHROTRA. Mobile Applications Usability Parameters: Taking an Insight View. In: *Information and Communication Technology for Sustainable Development*. Goa: Springer, 2018, pp. 35–43. ISBN 978-981-10-3932-4. DOI: 10.1007/978-981-10-3932-4_4.
- [40] MELICHER, W., D. KURILOVA, S. M. SEGRETÍ, P. KALVANI, R. SHAY, B. UR, L. BAUER, BAUER, N. CHRISTIN, L. F. CRANOR and M. L. MAZUREK. Usability and Security of Text Passwords on Mobile Devices. In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. San Jose: ACM, 2016, pp. 527–539. ISBN 978-1-4503-3362-7. DOI: 10.1145/2858036.2858384.
- [41] KO, L.-F., J.-C. LIN, C.-H. CHEN, J.-S. CHANG, F. LAI, K.-P. HSU, T.-H. YANG, P.-H. CHENG, C.-C. WEN, J.-L. CHEN and S.-L. HSIEH. HL7 middleware framework for healthcare information system. In: *HEALTHCOM 2006 8th International Conference on e-Health Networking, Applications and Services*. New Delhi: IEEE, 2006, pp. 152–156. ISBN 0-7803-9704-5. DOI: 10.1109/HEALTH.2006.246437.
- [42] MURUA, A., E. CARRASCO, A. AGIRRE, J. M. SUSPERREGI and J. GOMEZ. Upgrading Legacy EHR Systems to Smart EHR Systems. In: *International Conference on Innovation in Medicine and Healthcare*. Vilamoura: Springer, 2017, pp. 227–233. ISBN 978-3-319-59397-5. DOI: 10.1007/978-3-319-59397-5_24.
- [43] WELLS, B. and A. PENN. US09/799585. *System and method for interacting with legacy healthcare database systems*, 2003.
- [44] PARK, C.-Y., J.-H. LIM and S. PARK. ISO/IEEE 11073 PHD standardization of legacy healthcare devices for home healthcare services. In: *2011 IEEE International Conference on Consumer Electronics (ICCE)*. Las Vegas: IEEE, 2011, pp. 547–548. ISBN 978-1-4244-8712-7. DOI: 10.1109/ICCE.2011.5722731.
- [45] MYKKANEN, J., J. PORRASMAA, J. RAN-NANHEIMO and M. KORPELA. A process for specifying integration for multi-tier applications in healthcare. *International Journal of Medical Informatics*. 2003, vol. 70, iss. 2, pp. 173–182. ISSN 1386-5056. DOI: 10.1016/S1386-5056(03)00058-3.

About Authors

Zhongwei TENG is pursuing a Ph.D. in Computer Science in Vanderbilt University. His research interests include mobile security, cyber-physical systems and machine learning.

Peng ZHANG is an Assistant Professor in the Department of Mathematics and Computer Science at Belmont University. Her research interests include model-driven design for engineering and healthcare IT systems, decentralized algorithms and protocols for facilitating and securing clinical communications, and application and enhancement of Blockchain technologies for moving towards patientcentered care.

Xiao LI received her M.Sc. in Computer Science in Vanderbilt University.

William NOCK is an Research Assistant in Computer Science in Vanderbilt University.

Denis GILMORE attended medical school at Royal College of Surgeons in Dublin, Ireland. He

completed his general surgery residency at Beth Israel Deaconess Medical Center in Boston, MA. While in Boston, he completed a clinical fellowship in thoracic surgery at Brigham and Women's Hospital and research fellowship at Harvard Medical School. Dr. Gilmore continued his training by completing a cardiothoracic surgery fellowship at Vanderbilt University Medical Center in Nashville, TN. Dr. Gilmore specializes in the treatment of lung cancer, lung disease, lung nodules, esophageal disease, mediastinal adenopathy and pleural effusion.

Marcelino RODRIGUEZ-CANCIO was born in Santa Clara, Cuba. He received his M.Sc. from the University of Las Villas, Cuba in 2013 and his Ph.D. from the University of Rennes, France in 2017. His research interests include topics related to Machine Learning and Cyber Security.

Jules WHITE is an Associate Professor of Computer Science in Vanderbilt University. His research interests include mobile security, mobile augmented reality, cyber-physical systems, deployment and configuration optimization, distributed Systems and cloud Computing.

Jonathan C. NESBITT has been in the practice of thoracic surgery since 1989. He has broad experience in the management of thoracic diseases including lung cancer, esophageal cancer, minimally invasive surgery, diseases of the mediastinum, airway

tumors, airway stents, chest wall tumors and pleural diseases. He has extensive experience in resection of complex thoracic tumors including locally advanced cancers, reoperative surgery and multi-modality therapy. His interests also include minimally invasive approaches in the surgical management of thoracic diseases. His research has focused on the evaluation of multidisciplinary treatment for thoracic malignancies.

Douglas C. SCHMIDT is the Cornelius Vanderbilt Professor of Computer Science, Associate Provost for Research Development and Technologies, Co-Chair of the Data Sciences Institute, and a Senior Researcher at the Institute for Software Integrated Systems, all at Vanderbilt University. Dr. Schmidt's research covers a range of software-related topics, including patterns, optimization techniques, and empirical analyses of frameworks and model-driven engineering tools that facilitate the development of mission-critical middleware for Distributed Real-Time Embedded (DRE) systems and mobile cloud computing applications running over wireless/wired networks and embedded system interconnects. He has published 12 books and more than 600 technical papers – many in top conferences and journals. Dr. Schmidt received B.A. and M.A. degrees in Sociology from the College of William and Mary in Williamsburg, Virginia, and an M.S. and a Ph.D. in Computer Science from the University of California, Irvine (UCI) in 1984, 1986, 1990, and 1994, respectively.