A mobile-based architecture for integrating personal health record data

Muhammad H. Aboelfotoh
School of Computing
Queen's University
Kingston, Ontario
mha@cs.queensu.ca

Patrick Martin
School of Computing
Queen's University
Kingston, Ontario
martin@cs.queensu.ca

Hossam S. Hassanein
School of Computing
Queen's University
Kingston, Ontario
hossam@cs.queensu.ca

***Abstract*—Personal Health Record (PHR) systems provide patients with access to their own records, as well as control over who accesses their record. There are many PHR system providers available on the market. These PHR systems, however, have little means to integrate with healthcare facilities in the healthcare system network. This paper proposes a Personal Health Record (PHR) system solution which allows for exchange of patient data at the point-of-care using the patient's mobile device. The objective is to outline and address the issues that arise when adopting an hybrid PHR architecture that comprises a mobile component and an online remote server component. Preliminary tests are conducted in order to assess the system's usability.**

I. Introduction

Personal Health Record (PHR) systems have been introduced as the solution to empowering the general public by giving people a place to store and access their health data. PHR systems may be offered by private or public healthcare institutions, IT vendors, or health insurance companies for filing insurance claims. They essentially provide patients with a personal online profile with privacy controls, allowing the patient to control who has access to their health record [1].

Steele et al. [2] categorize different PHR system architectures from different perspectives. From the perspective of the location of the health record itself, PHR system architectures can be categorized as local, remote, and hybrid. Local storage location refers to the health record being accessible to the physician via local storage such as USB storage, a smartcard, or a mobile device. Local storage locations require no internet connectivity. A remote storage location refers to some online server or cloud-based service that provides access to patient health data. Remote storage locations require continuous connectivity. A hybrid storage approach uses a combination of both local and remote storage locations. Hybrid approaches require intermittent connectivity. Steele et al. do not propose any particular architecture but recommend a hybrid approach. In addition, they outline several requirements for such an approach. Such hybrid solutions already exist in the market [3]. Those solutions, however, are not networked with the healthcare system and so are not fed health record data from the healthcare system.

The first problem is to find a suitable hybrid architecture for such a system. One can realize such an architecture by the use of a device that supports communication and storage capabilities, such as increasingly ubiquitous consumer mobile devices. By using a mobile PHR, one does not require that healthcare facilities maintain online repositories of patient data with 24-hour uptime. In addition, data exchange agreements between healthcare facilities would be simplified as fully-internetworked healthcare facilities will no longer be mandatory. However, there are several issues with storing a patient's PHR on their mobile device:

PHR Data Integrity How do you ensure that sensitive details in the PHR can only be modified by authorized personnel? Introducing such a solution adds to the existing issue of tampering with patient records by physicians; the patients, if in control of their own health records, may be able to tamper with the contents. Palmieri et al. [4] argue that patients may lie to avoid incarceration or other undesired legal consequences of their actions. With patients in control of their own records a patient may, for instance, tamper with their personal health record to modify lab test results to hide drug abuse.

Data Misinterpretation Sometimes physicians write personal notes or intermediary data concerning a patient. A patient's lack of knowledge and understanding of the contents of these notes can result in misinterpretations by patients. This can cause fear and stress, and can result in extra time spent on having to explain to the patient what the physician's notes mean [5]. Typical online PHR systems provide a portal for the patient and a separate portal for the physician. Implementing a feature that restricts a certain section of the patient record to physician access is relatively straightforward. By using the patient's device, however, we lose control of the infrastructure, and so implementing such feature is not as trivial.

Mobile PHR Security The patient's mobile device might be running malicious applications, or may fall into the hands of someone with malicious intent. A person with malicious intent who can read the mobile PHR should not be able to learn anything about its contents.

In addition, relying on the mobile device to store the PHR can be problematic if the mobile device is lost. Another issue is that physicians may need to access the PHR outside the patient visit. These issues can be addressed by having a replica on an online PHR system. However, the following issues then arise:

Privacy The second problem is to provide privacy to the individuals who store their health information on the PHR system. This PHR system therefore must have means to secure access to patient data. There must also be mechanisms to minimize the impact of data leakage or a security breach, should it happen. Also, the PHR should be protected from unauthorized access even by system administrators or main-

978-1-4799-6644-8/14/$31.00 ©2014 Crown

tainers. PHRs may contain sensitive data related to sexually transmitted diseases, behavioral or mental health services, or treatment for alcohol and drug abuse. An insider operating the PHR system may use or aid in using this information for malicious purposes. By encrypting the PHR, one can hinder unauthorized attempts to read the PHR. However, if we are to allow different entities to access different parts of the PHR, then we require means to manage this encryption.

Given these issues we derive the following set of requirements for our system:

- **R1** The system must ensure integrity of any data entered by a physician.
- **R2** The system must provide the ability for a physician to store notes in part of the PHR which is only accessible by physicians.
- **R3** Unauthorized access of the mobile device should not allow for disclosure of information contained within the PHR stored on the mobile device
- **R4** The patient must be able to control who has access to their PHR. Any entities operating systems used for storing the PHR and that are outside the patient's control, but are not data sources (e.g. PHR system administrators), are no exception.

Previous research on the use of mobile devices for communicating personal health data tend to discuss aspects relating to functionality and utility [6], as well as social aspects [7,8]. However, they mostly do not discuss architectural details. HealthPass [9,10] is a mobile-based PHR system that enables the exchange of PHR data with a physician at the point-of-care. The system uses a Health Certificate Authority to authenticate the entity (e.g. physician) accessing the mobile PHR. For access to the mobile PHR, the system uses a Health Certificate Authority to enable the patient and physician to verify and validate each other. The main focus of Steele and Min [10] is to define fine-grained access control to the mobile PHR. Various sensitivity levels are associated with different sections in the PHR. Access control rules are defined in an XML-based format. One issue with HealthPass is that it trusts the patient's mobile device in enforcing access control to the entire PHR. Therefore implementing a section on the mobile device that can only be accessed by a physician is not promising. In this case requirement R2 is not met. Also, there was no discussion on security and privacy in the case of e.g. lost mobile device. Therefore requirement R3 is not met. HealthPass proposes means to express access permissions to different parts of the PHR, thereby somewhat addressing requirement R4. However, there's no detailed discussion on how this would be implemented or enforced by the system. The other issue is that there is no discussion on how a mobile PHR would work with an online PHR. Our contribution intends to address our derived set of requirements.

The remainder of this paper is organized as follows. Section 2 describes the system architecture, and how our system addresses each of the issues discussed earlier. Section 3 describes preliminary tests on some aspects of our system. Finally, Section 4 concludes our work and discusses future work.

II. Proposed system

An overview of our proposed system architecture is shown in Figure 1. This system must allow patients to use the online PHR systems that they are subscribed to and simultaneously use their mobile devices to provide direct data access to physicians. Therefore a mobile application can link the mobile device with the online PHR system. Not every physician or healthcare institution is able to access the online PHR system to which the patient is subscribed so access to the mobile device of the patient may be required. There should be a backend infrastructure which provides authentication and data integrity. This infrastructure must be less complex than a fully interconnected healthcare systems network. With these design considerations in mind, the following system components are required:

Mobile device of patient The mobile device stores the patient health record. An application on the mobile device is responsible for synchronization of the patient health record between the mobile device and the PHR system.

PHR system The PHR system provides an online server which the patient can log into in order to view a replica of their record. This system also allows a physician to access the health record of a patient given the required access privileges.

Smart health card The health card of the patient is a smart card which serves as part of an authentication process required to access the health record from the mobile device of the patient.

Healthcare Provider (HCP) terminal This typically is a desktop computer equipped with a smart card reader/writer, Near Field Communication (NFC), Bluetooth/WiFi. This terminal is used to perform reads and writes to the mobile PHR. The terminal resides in a healthcare facility, at a physician or receptionist's desk, and connects to the patient's smart card and mobile device. This terminal is also connected to the backend infrastructure used for authentication.

Physician registry We assume that every physician has a registration number. This registration number identifies the physician as an official healthcare practitioner. This system already exists in some countries such as the United States and Canada. In addition, means to perform an online lookup on physician information is provided. For instance, the College of Physicians and Surgeons of Ontario provides a website from which one can search for a registered physician by name or registration number [11]. We require a unique public key associated with each physician that is stored along with the other information found in the physician registry. The physician uses their private key to digitally sign their updates to the PHR. The physician registries may expose Web Services to provide lookup services, to ease interoperability with other systems that require such information.

The health record The Personal Health Record (PHR) is essentially a set of HL7 Continuity of Care Documents (CCD) [12]. A single document may comprise many sections. The first section is the Header section that contains the name and birth date of the patient. The Alerts section comprises allergy information. The Medications section comprises a history of medications prescribed to the patient. The Results section comprises clinical findings, such as lab test results. Different sections in the CCD such as the Medications section, are composed of entries, each entry is defined by the XML element 'entry'. For example, each 'entry' element in the 'Medications'

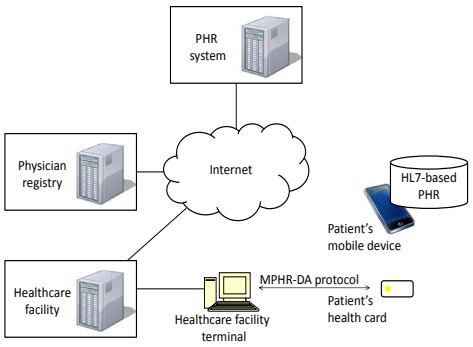


Fig. 1: System architecture

section corresponds to a medication on the patient's record. Each 'entry' element has an 'id' subelement with a 'root' attribute that represents a unique identifier for that entry. PHR data sources can be categorized as a) Patient-entered data, which includes manually entered data or data from biological sensors; b) Physician data: this is data typically entered by physicians during encounters, and c) Lab data: the online PHR may be connected to labs which may transmit lab test results directly to the online PHR system.

A. PHR data integrity

We need to ensure that illicit modifications made to data entered by physicians do not go undetected. This is achieved by signing physician record entries with the physician's key. An entry is stored using the W3C XML Signature standard and the XML signature element is inserted as part of the HL7 CDA Actor element. This Actor element follows the element signed in the patient record. A physician reading record entries verifies the signed entries to ensure that it has been entered by a certified physician. A SHA-1 hash is calculated on the entry, which is then digitally signed by the physician. The physician's public key would be fetched using the URI specified in the Signature element.

Document management Initially, when a patient retrieves an electronic version of their health record, they may receive a single CCD document signed by a physician. This document may be addended as the patient makes visits to clinics. The addendums contain the latest observations from these encounters. At some point in time, the patient may agree to fixing an inaccuacy in the first document. If this is the case, then the addenda documents must be updated to refer to the new document as the parent document.

B. Mobile PHR sections with physician-only access

We employ a symmetric key algorithm such as the Advanced Encryption Standard (AES) [13] to enable a physician to encrypt entries they do not wish the patient to view immediately, but perhaps after consultation. An entry is enveloped in an XML Encryption EncryptedData element [14]. XML Encryption is a standard for transferring encrypted data. The EncryptedData element also holds information such as the encryption method (e.g. AES-128-CBC). The KeyName parameter is used to associate an identifier with the AES key used to encrypt the entry contents. The key is stored on the patient's health card. The identifier is used to look up and fetch the key from the patient's health card using a security protocol. This protocol is used to access the keys stored on the patient's health card. The protocol utilizes the physician registry in ensuring that the entity requesting access is a certified physician.

Mobile PHR Direct Access (MPHR-DA) protocol We briefly introduce our proposed MPHR-DA protocol. This protocol is a work-in-progress and we plan on reporting more details in the future. Interactions in the protocol consist of three parts, namely request message, authentication, request execution. Interactions are initiated by the HCP terminal. The request message types available are 1) Set patient key: this sets the signature public key of the patient and pairs it with the patient's mobile device (the key is used to provide e-consent, described later), 2) Key read request: this requests reads a key stored on the health card, and 3) Key write request: this request writes a key stored on the health card. Both key request messages involve specifying and locating the key requested in the card directory. After the health card receives the request it sends a token which only the smart card and the entity issuing the health cards (e.g. ministry of health) can understand. This token is encrypted and forwarded by the healthcare facility, along with physician and healthcare facility identification, to a backend provided by the issuer for authentication. The backend uses the physician registry to look up the physician's public key for verification and decryption of the forwarded token.

C. Mobile PHR security

If the patient's mobile device is lost or stolen, someone with malicious intent may be able to access the mobile PHR. Therefore the mobile PHR must be encrypted so no one can learn anything from the contents of the health record. Akinyele et al. [15] propose a mobile PHR that employs attribute-based encryption (ABE) to control the privacy of the PHR. The issue with this approach is that the ABE-encrypted record and the decryption keys are both stored on the mobile device. The keys are encrypted with a random passphrase provided by a hospital administrator. We can also authenticate the patient using other authentication factors, such as biometrics (e.g. fingerprints) to protect the mobile PHR. For instance, a passphrase could be used to generate a key using a key derivation function [16]. Whenever the patient instructs the mobile PHR to provide access, the derived key would then be used to perform on-demand encryption/decryption of the mobile PHR using AES. In this case, the entire HL7 CCD, as well as the root key and secret key would be encrypted using AES and a derived key.

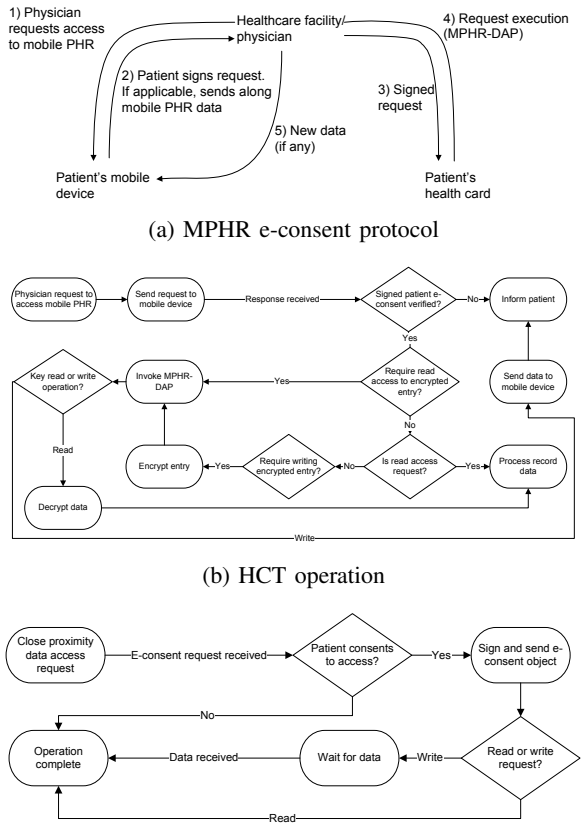
One can also utilize trusted hardware security features found in some mobile platforms, as suggested by Dmitrienko et al. [17]. These features could be used to implement a trusted platform. This trusted platform would provide an application with protection from tampering by malicious applications that may reside on the mobile device. In addition, the trusted platform would provide secure storage for sensitive data, to protect against direct read access attempts by those of malicious intent. Dmitrienko et al. propose such a system to provide a healthcare professional with secure mobile access to

an EHR system. In our system, this could be used to protect the mobile PHR and the keys used to decrypt the mobile PHR.

D. Privacy

We require means to preserve the confidentiality of the mobile and online PHR. Encrypting the PHR requires us to provide means to manage this encryption in a way that allows physicians access to this PHR, given the patient's permission. Benaloh et al. [18] propose a scheme that allows patients to share partial access rights of their PHR, and to perform searches over an encrypted PHR. They model the health record as a hierarchy of categories. For instance, a 'Basic Medical Info' category contains the leaf categories 'Allergies' and 'Medications'. To provide access to a physician, the patient first generates a root key from which decryption keys for any category can be generated. Then the patient selects a subset of the categories to be accessed. A single key for that subset is issued. This single key can be used to generate encryption/decryption keys for all the categories in the subset. Similar to Benaloh et al., the PHR system client application residing on the devices of patients uses pseudonyms to register patients. The client application transparently handles allocating a new pseudonym when registering with the PHR system. The name of the patient is only disclosed to the physician given consent to access the patient's record. Patients need to be able to describe what they permit (or forbid) physicians to do when accessing their PHR data. This includes which parts of the PHR the physician is allowed to access, as well as the duration for access. This is known in the literature as providing electronic consent (e-consent) [19–21]. When a physician or healthcare facility requests access to a patient's PHR, the patient provides the requesting entity with e-consent. This e-consent dictates the nature of the access allowed, such as time period of access, reason, etc. In some cases, some information about the entity that requires consent (e.g. physician ID) may not be known in advance. To this end, Asghar and Russello [20] propose the use of templates to describe the consent in advance, and when the required information is available the consent management system instantiates the necessary access policies from these templates.

E-consent object Patients provide permission to access the PHR by providing an e-consent object, which captures the consent parameters. For describing the consent, we propose adopting the use of templates as in Asghar and Russello's [20] approach. The e-consent contains information such as the healthcare provider's identifier, requested record sections, reason for access. In addition, since we are adopting the privacy scheme proposed by Benaloh et al. we require that any keys the physician requires are included as part of the e-consent object. Furthermore, HL7 has published an implementation guide for Privacy Consent Directives [22]. This guide defines HL7 document element types to be used for transferring privacy consents. We incorporate the e-consent object proposed by Asghar and Russello into the HL7 privacy consent object which contains HL7-defined parameters such as ActConsentType and PurposeOfUse. ActConsentType specifies the action being consented to. Examples of HL7 ActConsentTypes are information disclosure (IDISCL), access and save only (INFASO). PurposeOfUse specifies the reason for performing actions on the information. Examples are treatment (TREAT), emergency treatment (ETREAT). A similar example of the use of HL7 CDA for describing privacy consent has been shown by Ko and Liou [23]. For details on other attributes consult the HL7 Privacy Consent Directives document [22].



(a) MPHR e-consent protocol

(b) HCT operation

(c) Mobile device operation

Fig. 2: MPHR e-consent protocol execution and device operation

Mobile PHR (MPHR) e-consent protocol Figure 2a illustrates the process of providing e-consent and accessing the mobile PHR, assuming a typical outpatient setting. Figure 2b and Figure 2c respectively illustrate how the healthcare facility terminal and the patient's mobile device operate. At the beginning of the patient visit, the physician initiates a request to access certain parts of the mobile PHR. This request is sent from the healthcare terminal (HCT) to the patient's mobile device. The patient approves the request presented to them on the mobile device. The mobile device then signs the request using the patient's signature key, and sends the response, along with the requested data, to the HCT. If physical docking is not an option, technology similar to Android Beam [24] or S-Beam [25] for seamlessly connecting mobile and desktop platforms can be used to connect the mobile device to the HCT. Both technologies use NFC for connection setup and automatic pairing, and either Bluetooth (Android Beam) or WiFi-Direct (S-Beam) as a backhaul connection. This allows for transferring larger amounts of data than the typical NFC tag data. Both technologies support automatic pairing between two devices. Towards the end of the patient visit, the physician may need to write data to the MPHR, some of which may reside in a physician-access-only part of the health record. The part which requires physician-access invokes the MPHR-DA protocol in

order to obtain the key to decrypt/encrypt that part. The other data, however, is sent to the patient's mobile device. In either case, the physician signs the update made to the MPHR. If the physician has access to the patient's online PHR system and requires access outside the patient visit, an e-consent object can be obtained from the patient either during the visit or from the online PHR system.

III. Preliminary tests

In order to evaluate the viability of our proposed system we have conducted preliminary experiments. Results are shown in Figure 3. Our concern in the experiments is how much time the system spends in the clinical workflow. We performed our experiments on a laptop with a 2.66 GHz Intel Core 2 Duo processor running Mac OS X 10.6 with 4GB of RAM, and an internal Bluetooth adapter. This represents the terminal at the healthcare facility, such as the receptionist's or the physician's computer. As for the patient's mobile device, we used a Samsung Nexus S (ARM-based processor) running Android 4.1.2 with 512MB of RAM. We note that this architecture can be ported to other operating systems. The parser application running on the laptop was implemented using the Java DOM, whereas on the mobile device the application was implemented using XMLPullParser. To further illustrate, we assume a typical outpatient scenario given the outpatient setting described previously, and discuss how our system would be utilized.

Outpatient test scenario. A patient arrives at a clinic for an appointment with a physician and checks in at the reception desk. At this stage if the physician has pre-specified the required parts of the PHR that need to be accessed, then the MPHR access steps (see Figure 2) can be carried out at this stage. The patient is instructed to wait for the physician until the physician is ready to see the patient. At the beginning of the encounter with the physician, the physician reads the patient's PHR. During the encounter the physician takes notes. At the end of the encounter the physician wants to update the patient's mobile PHR, and add data to the physician-only access section of the PHR. The physician requests the patient's health card and invokes the MPHR-DA protocol. The physician's observations and notes are sent from the physician's terminal to the patient's mobile device and the patient is discharged. During the patient's encounter with the physician, the physician reads the patient's PHR at the beginning of the encounter and his/her observations at the end of the encounter. The mobile device updates the online PHR with the modifications made to the mobile PHR. This is done either asynchronously or by explicit synchronization, depending on the patient's preferences.

Results From the outpatient scenario we described, we define variables introduced by our solution, that may affect system usability. Our main concerns are how increasing the size of the mobile PHR clinical documents affects the transfer and processing time of these documents at a healthcare facility. For different document sizes, the variables measured are the amount of time it takes to parse, sign/verify documents on both a mobile device (patient's mobile PHR) and a desktop platform (physician's terminal), as well as encryption/decryption of document data on a desktop platform. In addition, we measured the Bluetooth transfer time between the mobile device and the desktop platform. The results in Figure 3 show that the time consumed by encryption/decryption, and signing/verifying of mobile PHR clinical documents is negligible with respect to bluetooth transfer and parsing on the mobile device. Bluetooth transfer time may be perceived as an issue with larger-sized health records. However, we note that data transfer between the patient's device and the healthcare provider occurs in the initial stage of an outpatient scenario, and at the end of the encounter with the physician. In the initial stage, the data transfer could be completed while the patient is waiting for the physician. In the second data transfer, it is assumed that, in general, the size of the update by the physician would be much smaller than the size of the data read from the health record. For a single 4MB clinical document, the system overhead ranges from 2.5 seconds (no encrypted sections) to 2.7 seconds (entire document encrypted), excluding transfer time. With transfer times, the minimum system overhead ranges from 27.2 (no encrypted sections) to 27.4 seconds (entire document encrypted). Transfer time consumes 90% to 91% of the total overhead time.

IV. Future work and conclusion

One of the issues that may be faced is the limited PHR storage space on a mobile device. One solution could be the application of a minimum, a threshold, and maximum for the storage space used by the MPHR. In the case where the MPHR may run out of space, superceded clinical document versions could be backed up and removed from the mobile storage. Furthermore, data management issues may need to be explored, especially when multiple backup storage devices of different forms are used. We are currently working on a security assessment of the MPHR-DA protocol, as well as system evaluation, and an ecosystem for improving the quality of personal health records.

To conclude, we outlined issues that need to be addressed when adopting a hybrid architecture for PHR systems. From these issues we derived a set of requirements for a hybrid architecture. We discussed a similar system and highlighted the observed shortcomings in meeting these requirements. From that, we proposed a system which addresses those requirements. Our proposed architecture provides the ability to allocate parts of the mobile PHR which are only accessible by physicians. We conducted a preliminary evaluation of the system in order to observe how much overhead the mobile PHR would introduce.

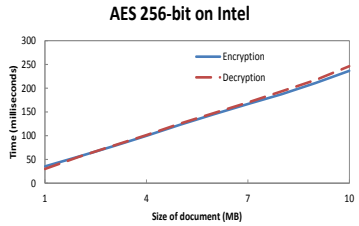
References

[1] P. C. Tang, J. S. Ash, D. W. Bates, J. M. Overhage, and D. Z. Sands, "Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption," *Journal of the American Medical Informatics Association*, vol. 13, no. 2, pp. 121–126, 2006.

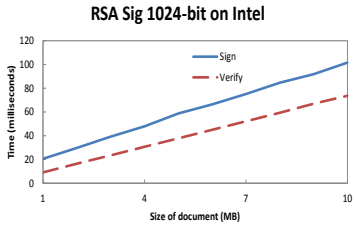
[2] R. Steele, K. Min, and A. Lo, "Personal health record architectures: Technology infrastructure implications and dependencies," *Journal of the American Society for Information Science and Technology*, 2012.

[3] "mihealth," Available at: https://mihealth.com/. Last accessed November 20, 2012.

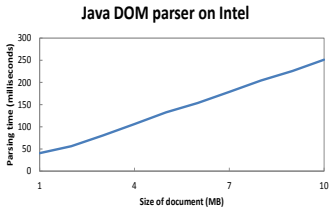
[4] J. J. Palmieri and T. A. Stern, "Lies in the doctor-patient relationship," *Primary care companion to the Journal of clinical psychiatry*, vol. 11, no. 4, p. 163, 2009.



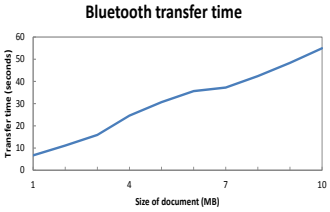
(a) Encryption/decryption times of a single HL7 CCD of different sizes



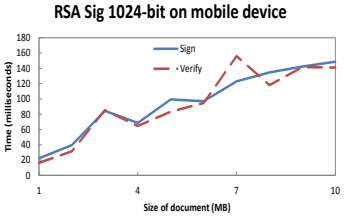
(b) Signing/verifying times of a single HL7 CCD of different sizes



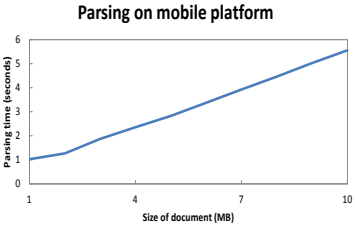
(c) Parsing of a single HL7 CCD of different sizes



(d) Bluetooth transfer time of a single HL7 CCD of different sizes



(e) Signing/verifying times on mobile device



(f) Parsing times on mobile device

Fig. 3: Experimental results

[5] R. van der Vaart, C. H. Drossaert, E. Taal, and M. A. van de Laar, "Giving rheumatology patients online home access to their electronic medical record (EMR): advantages, drawbacks and preconditions according to care providers," *Rheumatology international*, vol. 33, no. 9, pp. 2405–2410, 2013.

[6] M. I. Kim and K. B. Johnson, "Personal health records evaluation of functionality and utility," *Journal of the American Medical Informatics Association*, vol. 9, no. 2, pp. 171–180, 2002.

[7] J. Sarasohn-Kahn, *How smartphones are changing health care for consumers and providers*. California HealthCare Foundation, 2010.

[8] R. Steele, "Social media, mobile devices and sensors: categorizing new techniques for health communication," in *Fifth International Conference on Sensing Technology (ICST)*. IEEE, 2011, pp. 187–192.

[9] R. Steele and K. Min, "Role-based access to portable personal health records," in *MASS'09. International Conference on Management and Service Science*. IEEE, 2009, pp. 1–4.

[10] R. Steele and K. Min, "Healthpass: Fine-grained access control to portable personal health records," in *24th IEEE International Conference on Advanced Information Networking and Applications (AINA)*. IEEE, 2010, pp. 1012–1019.

[11] "The college of physicians and surgeons of Ontario," available at: http://www.cpso.on.ca. Last accessed January 5, 2013.

[12] Health Level Seven International, "HL7/ASTM implementation guide for CDA R2 - continuity of care document (CCD) release 1," April, 2014. Available: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=6.

[13] F. P. Miller, A. F. Vandome, and J. McBrewster, *Advanced Encryption Standard*. Alpha Press, 2009.

[14] "XML encryption syntax and processing version 1.1," Internet: http://www.w3.org/TR/2013/REC-xmlenc-core1-20130411/, Apr. 11, 2013 [Dec. 09, 2013].

[15] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. Peterson, and A. D. Rubin, "Securing electronic medical records using attribute-based encryption on mobile devices," in *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, 2011, pp. 75–86.

[16] F. F. Yao and Y. L. Yin, "Design and analysis of password-based key derivation functions," in *Topics in Cryptology–CT-RSA 2005*. Springer, 2005, pp. 245–261.

[17] A. Dmitrienko, Z. Hadzic, H. Löhr, A.-R. Sadeghi, and M. Winandy, "Securing the access to electronic health records on mobile phones?" *Biomedical Engineering Systems and Technologies, Springer-Verlag, Ed*, 2011.

[18] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: Ensuring privacy of electronic medical records," in *Proceedings of the 2009 ACM Workshop on Cloud Computing Security*, ser. CCSW '09. New York, NY, USA: ACM, 2009, pp. 103–114. [Online]. Available: http://doi.acm.org/10.1145/1655008.1655024

[19] C. Pruski, "e-crl: A rule-based language for expressing patient electronic consent," in *Second International Conference on eHealth, Telemedicine, and Social Medicine, 2010. ETELEMED '10*, 2010, pp. 141–146.

[20] M. R. Asghar and G. Russello, "Actors: A goal-driven approach for capturing and managing consent in e-health systems," in *International Symposium on Policies for Distributed Systems and Networks (POLICY)*. IEEE, 2012, pp. 61–69.

[21] O. Can, "A semantic model for personal consent management," in *Metadata and Semantics Research*. Springer, 2013, pp. 146–151.

[22] Health Level Seven International, "HL7 implementation guide for CDA release 2: Privacy consent directives, release 1," May, 2013. Available: http://gforge.hl7.org/gf/download/frsrelease/977/10295/CDAR2_IG_CONSENTDIR_R1_N1_2013MAY.pdf.

[23] Y.-Y. Ko and D.-M. Liou, "The study of managing the personal consent in the electronic healthcare environment," *World Academy of Science, Engineering and Technology*, vol. 65, p. 314, 2010.

[24] "NFC basics — Android developers," Internet: http://developer.android.com/guide/topics/connectivity/nfc/nfc.html, [Dec. 09, 2013].

[25] "What is S Beam™, and how do I use it on my Samsung Galaxy S® III?" Internet: http://www.samsung.com/us/support/supportOwnersHowToGuidePopup.do?howto_guide_seq=7042&prd_ia_cd=N0000003&map_seq=48157, Nov. 22, 2013 [Dec. 09, 2013].