2015

Security of eprescription: Security of data at rest in prescription exchange services vs on mobile devices

Kyaw Kyaw Htat
Edith Cowan University

Patricia A. H. Williams
Edith Cowan University

Vincent McCauley
Edith Cowan University

DOI: 10.14221/aeis.2015.2
4th Australian eHealth Informatics and Security Conference, held from the 30 November – 2 December, 2015 at Edith Cowan University, Joondalup Campus, Perth, Western Australia.

SECURITY OF EPRESCRIPTION: SECURITY OF DATA AT REST IN PRESCRIPTION EXCHANGE SERVICES VS ON MOBILE DEVICES

Kyaw Kyaw Htat[1], Patricia A H Williams[1,2,4], Vincent McCauley[3,4]
[1]School of Computer and Security Science, [2]Security Research Institute, Edith Cowan University
[3]Integrating the Healthcare Enterprise (IHE) Australia,
[4]Health Level 7 (HL7) Australia
khtat@our.ecu.edu.au, trish.williams@ecu.edu.au, vincem@mccauleysoftware.com

Abstract
One area of healthcare that has moved more quickly than others in adopting electronic transfer of information is prescribing in the primary care environment. Several Acts and Regulations have been repealed and amended at Commonwealth and State levels to enable this progress over the past decade, as medication provision is a strictly controlled area of healthcare. Further, numerous standards and specifications have been developed and adopted to support and safeguard the regulatory changes and facilitate the electronic transfer of prescriptions. However, the current model of electronic prescription transfer comes with a substantial price tag for ongoing use. With the Nation's growing and aging population, the number of prescriptions will increase annually, and thus it is necessary to find more cost-effective alternatives with comparable security and privacy assurances. An obvious potential solution lies in using devices that have been a part of our daily lives for well over a decade - mobile smartphones. An investigation was conducted to determine whether or not such technology is capable of meeting legislative requirements for prescribing whilst providing a cost-effective alternative prescription transfer model. Using technology such as near field communication for transfer process together with existing encryption technique demonstrates this can meet the security requirements of data at rest. This investigation established that although the proposed alternative is a work in progress and not a flawless one, it indeed opens up opportunities to incorporate many useful features in addition to eliminating the associated ongoing costs while providing comparable privacy and security assurances.

Keywords
ePrescription transfer, ePrescription security, mobile transfer of ePrescription, PES, eTP

INTRODUCTION

As much as eHealth plays a major role in the nation's journey towards improved and better maintainable healthcare system, electronic prescription transfer (eTP) facilitates eHealth itself as one of a few fundamental enablers. Current implementation of the electronic prescription system in Australia makes use of one of two prescription exchanges services (PES) from two different vendors/providers: *script exchange* from eRx and *script vault* from MediSecure. Despite their critical involvement in current implementation of eTP, on-going use of these PES comes with a high price tag as each eligible electronic prescription download incurs a $0.15 fee. Whilst this amount per prescription may sound trivial, the huge volume of prescriptions will results in a significant impact on the nation's healthcare expenditure in the long run. A recent announcement made by eRx regarding their dispensing of the first billionth electronic prescription (McDonald, 2015) is evidence that this approach has cost the nation $150 million to this point. It was only one of the two PES services making this announcement and the total electronic prescription fees incurred so far for the use of both PES services is likely to be significantly more, if not twice as much. Currently this electronic prescription fee has been subsidised by the Commonwealth through a series of Community Pharmacy Agreements, yet this significant on-going cost prompts the exploration of cheaper or more cost effective alternatives with comparable security measures.

One potential alternative to using PES services for transferring electronic prescription, is the use of a patient's mobile device as the transfer media/mechanism. This paper assesses and compares the security of the 'data at rest' in the current PES-based approach to that of a solution using mobile devices. This paper also presents the requirements, mandated by various specifications, for the security of electronic prescriptions in a consolidated and comprehensible form. It is a complementary work built on the previously published article on devising an alternative solution for the current eTP process (Htat, Williams, & McCauley, 2015). Despite being a work in progress towards devising a cost-effective/cheaper alternative with comparable security and privacy assurances for electronic prescription transfer, this paper delves further into technical discussion from the information security standpoint whilst the prior work focused on the viability of the alternative solution from legislative and regulatory perspectives. A future paper will compare and contrast the detailed security issues since this one merely describes learning from initial research and prototyping, not a complete implementation.

SECURITY OF DATA AT REST USING PES

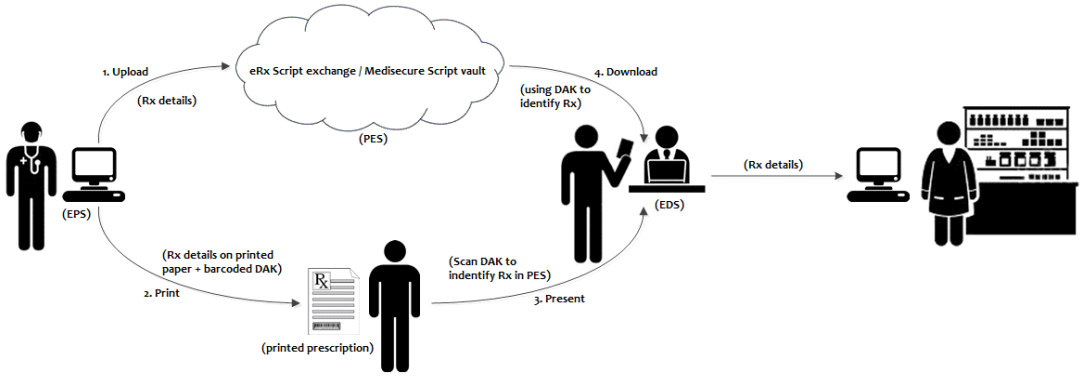

Figure 1: Current electronic prescription transfer model using PES (Htat, Williams, & McCauley, 2015)

Figure 1 briefly describes the current electronic prescription transfer model in Australia using PES. In this approach, ensuring the security of electronic prescriptions on PES services is primarily governed by the Australian Technical Specification (ATS) 4888 series, with 4888.2-2013 particularly emphasizing the platform independent model. Although the specification mentions that the security and confidentiality of data-in-transit is specific to the implementation platform, it covers detailed requirements for the security of data-at-rest on PES services. The security and confidentiality mechanism in eTP revolves around the concept of using a Document Access Key (DAK), which is presented as a barcode on the printed prescription created by any eTP enabled electronic prescribing system. In the current electronic prescription transfer model using a PES, the DAK is used for authorizing access to the prescription stored on the PES, for encrypting it prior to uploading and for decrypting it after downloading it from the PES. The ATS 4888.2-2013 (Section 5.3) provides an overview of the security mechanism implemented using the DAK for protecting the Secured Clinical Documents (i.e. prescriptions in this case). Figure 2 illustrates how this works.

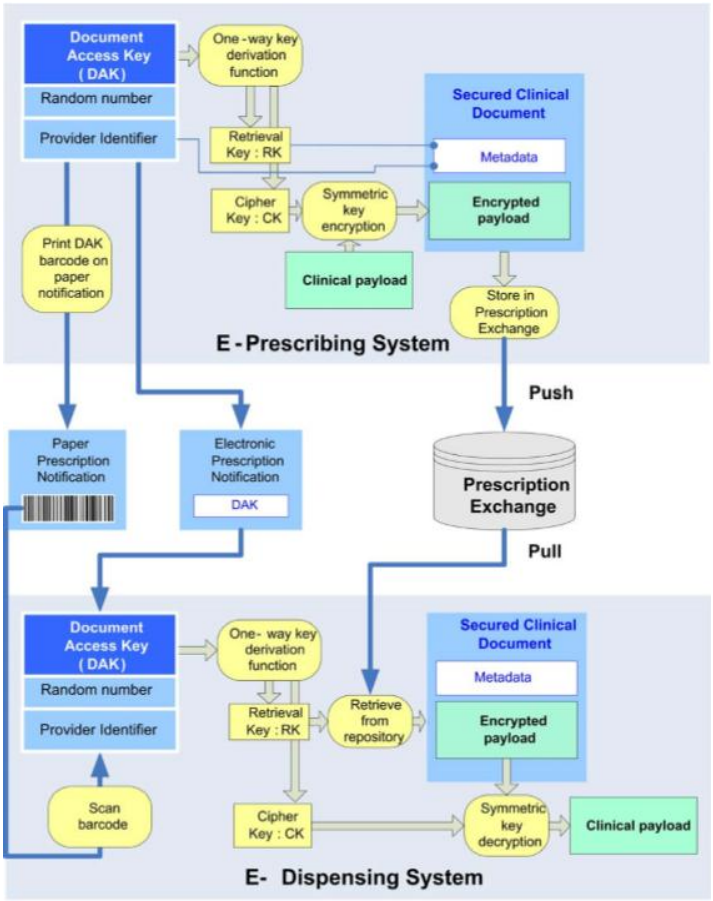

Figure 2: DAK usage for storage and retrieval of prescription with PES (Standards Australia, 2013, Figure 19)

The DAK is a parent key from which all other keys such as *Retrieval Key*, *Cipher Key* and *DAK Holder Proof Key* are derived, using a published algorithm. Each DAK contains a *Provider ID* which uniquely identifies the operator/provider of the PES service and an entropic random value from which all other key are derived. The *Retrieval Key* (RK) is a random value which references a specific Secured Clinical Document (i.e. a prescription) from the PES once it is qualified with the *Provider ID*. Due to the fact that the random value of the DAK has sufficient entropy, it is impractical for someone to have a knowledge about it unless it is explicitly disclosed to that party. Therefore, possession of a Qualified RK acts as a bearer credential and thus grants the holder the right to retrieve the Secured Clinical Documents associated with that Qualified RK. The *Cipher Key* is a unique symmetric key generated using one-way function from the DAK and is used in encrypting and decrypting the payload/content of the Secured Clinical Document. This encryption of the prescription by the electronic prescribing system is evident in Figure 2 prior to pushing/uploading it to the PES. Unlike the *Retrieval Key*, this *Cipher Key* is never disclosed to the PES, therefore ensuring the content of the Secured Clinical Document is not visible to the operators of the PES and the individual's private information is inaccessible. This also eliminates the need for prescription subjects (i.e. patients) having to consent to the operator of a Prescription Exchange having access to their private information. The *DAK Holder Proof Key* is another key derived from the DAK using a one-way function, and is used by a dispensing pharmacy to prove to the PES that it holds a DAK. Figure 3 portrays the implementation independent characteristics of a DAK; the primary pillar on which the entire eTP security is built upon.

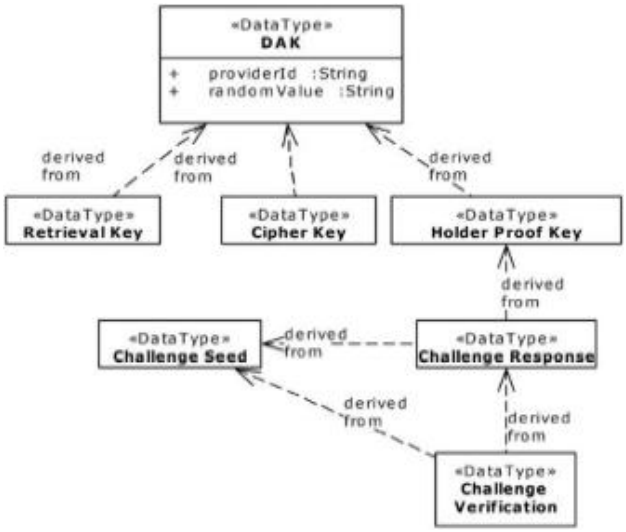

Figure 3: DAK and its constituent data types (Standards Australia, 2013, Figure 21)

To ensure the security of an electronic prescription on a PES, all of DAK's mandated characteristics are complemented by a list of security conformance points. Whilst the security of data in transit between eTP participants (i.e. *Prescriber*, *Prescription Subject*, *Prescription Exchange* and *Dispenser* etc.) relies on the encryption mechanism of the specific implementation platform, the security of data at rest makes use of the DAK for encryption within PES. When it comes to storing the DAK, or its derived *Cipher Key*, on any stable storage (i.e. a permanent storage), it is mandated to encrypt them with at least 128 bits encryption. In addition to this, derivation of any *Cipher Key*, *Retrieval Key* or *DAK Holder Proof Key* from a DAK by any system, is strictly prohibited unless the user of that system is authorised to access the information for the Prescription Subject of the Secured Clinical Document (i.e. the prescription) associated with that DAK. The specification ATS 4888.2-2013 also prohibits sharing of *DAK Holder Proof Key*, as well as storing it in any non-transient recoverable form. Figure 4 depicts the electronic prescription, the crucial piece of information, upon which the entire eTP system is built to support.

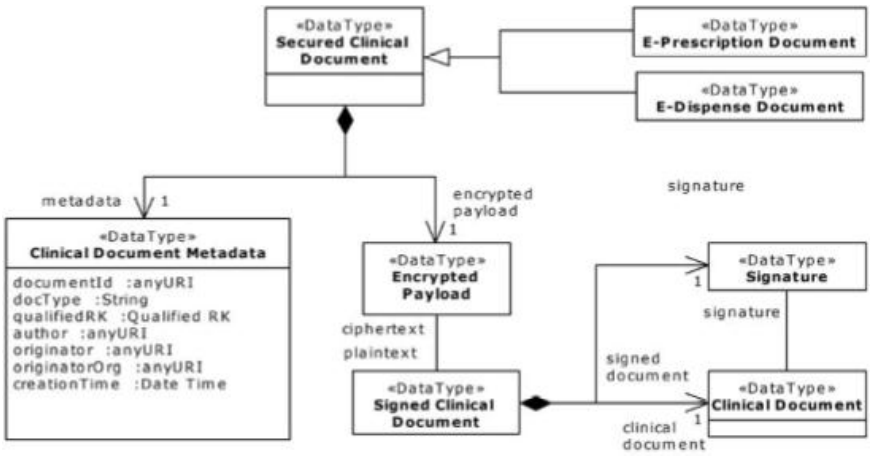

Figure 4: DAK and its constituent data types (Standards Australia, 2013, Figure 23)

Despite the specification ATS 4888.6-2013 being a platform specific implementation for web services, it outlines how the Secured Clinical Document is to be created for eTP or eHealth in general. The way in which a Secured Clinical Document is created has no direct impact on the security of data at rest on the PES. However, due to the resulting document type from this process, it is crucial in determining whether the use of mobile device for transferring electronic prescription is achievable. The specification mentions that the *Secured Clinical Document* is a *Signed Clinical Document* encoded as Base64 binary data within the *Message Payload* element in compliance with clause 7.3.1 of the specification ATS 5822-2010. In turn, the *Signed Clinical Document* is indeed an IHE's Cross-Enterprise Document Media Interchange (XDM) representation of an HL7 CDA form as defined in the specification ATS 4888.3-2013.

In general, the data at rest on the PES is strictly governed by a set of specifications and standards (i.e. such as HL7 CDA and IHE etc.) for its security and integrity, while facilitating the national transition towards eHealth.

SECURITY OF DATA AT REST USING MOBILE DEVICES

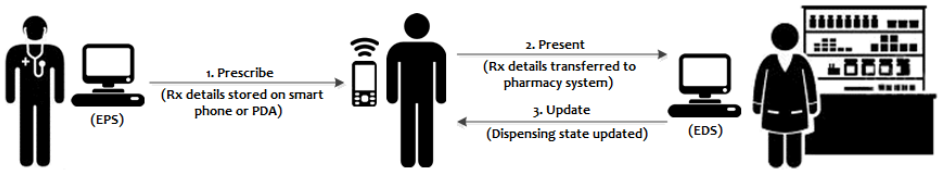

Figure 5: Electronic prescription transfer model using smartphones (Htat, Williams, & McCauley, 2015)

Figure 5 briefly depicts the proposed electronic prescription transfer model using patient's mobile smartphone. In this proposed alternative, the security of data at rest also makes use of DAK for encrypting the electronic prescription prior to transfer and decryption at the dispensing point. In this proposed approach, the electronic prescribing system transfer the encrypted prescription as well as its DAK to the mobile device for storage and transportation. The prescription will still be encrypted using DAK, in the same way as in the current approach using a PES. However, the encrypted prescription will then be stored on the mobile device instead of being uploaded to a PES. After this, the DAK itself will then be encrypted by the mobile electronic prescription transfer application using 128 bit symmetric encryption, which is in compliance with the section 7.3.3 Data Security Conformance points of the ATS 4888.2-2013 upon being stored on the mobile device. In this approach, the *Provider ID* part of the DAK, as well as the derived *DAK Holder Proof Key*, are not utilized as the prescription will not require the use of a PES and not be uploaded to a PES, thus it would no longer require proof of holding the DAK to any PES. The fact that *DAK Holder Proof Key* would no longer be required entirely eliminates the need to comply with the ATS 4888.2-2013's prohibition of *DAK Holder Proof Key* from sharing or storing in any non-transient recoverable form. The *Retrieval Key* and *Cipher Key* however will perform the same functions as in the prior approach using a PES. Figure 6 shows the new proposed electronic prescription transfer process.

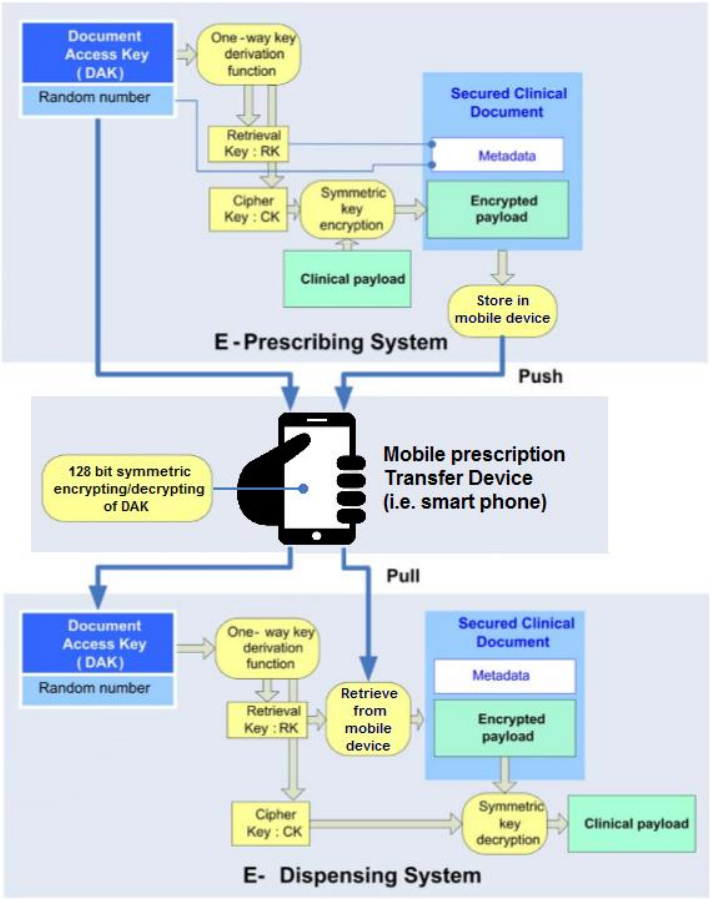

Figure 6: DAK usage for storage and retrieval of prescription in proposed approach

The proposed alternative is designed to use Near Field Communication (NFC) technology for the transfer of electronic prescription between the participant systems; the electronic prescribing system, the mobile device and the electronic dispensing system. Whilst there was consideration of other technologies such as Wi-Fi, Bluetooth and ZigBee, NFC technology was selected because of its design for close proximity communication and its well-received applications in areas such as mobile banking and card-less payment systems. In addition, NFC is a feature of many portable devices (i.e. especially in most smartphones) nowadays for transferring data from one device to another via a close proximity radio communication. Technically, it is a bidirectional high frequency (i.e. 13.56 MHz) radio communication technology operating at data transfer rate of 106 kbps, 212 kbps, or 424 kbps over the short distance of typically between 4 cm to 10 cm (ECMA International, 2013) for secure applications (Smart Card Alliance, n.d.).

For the security of the data in transit, the proposed approach relies on NFC's inbuilt security measures and its governing standards, in a similar manner the current PES approach relies on the specific implementation platform and relevant standards for the security of the data in transit. Among other relevant standards, the ISO/IEC 14443 (i.e. a four-part international standard for Contactless Smart Cards operating at 13.56 MHz in close proximity with a reader antenna), ECMA-340 and ECMA-352 from European Computer Manufacturers Association International (ECMA International) are a few primary governing standards for the NFC technology. Although the detailed study of the NFC technology and its security mechanism is beyond the scope of this paper, Figure 7 outlines its basic components and how it works in general.

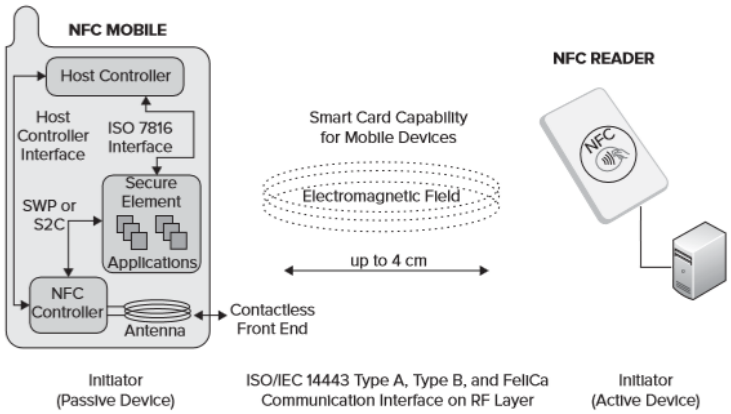

Figure 7: Basic anatomy of NFC (Coskun, Ok, & Ozdenizci, 2013, Figure 2-15)

Since the proposed approach does not utilize the *Provider ID* part of the DAK, as possession of the *Retrieval Key* alone acts as a bearer credential and grants the holder the right to access the Secured Clinical Documents associated with it. In the same way as in the approach using PES, the *Cipher Key* is never disclosed to the holder of the mobile device, who can potentially be a prescription subject's agent, thus eliminating further complication from an information privacy perspective. Furthermore, this approach firmly complies with the Data Security Conformance points stated in the section 7.3.3 of the ATS 4888.2-2013 to the same extent as the existing approach using a PES does. This compliance results not only in the electronic prescription but also the DAK, and any of its derived keys, being encrypted with 128 bits symmetric encryption upon to being stored on the mobile device.

As the mobile device replaces the PES for transferring prescriptions in the proposed approach, it will potentially hold multiple current/active prescriptions belonging to the same person at the same time. Therefore, the electronic prescription transfer application on the mobile device is envisaged to have a screen/page, characterised in Figure 8, in order to select prescriptions to be transferred to the electronic dispensing system for dispensing.

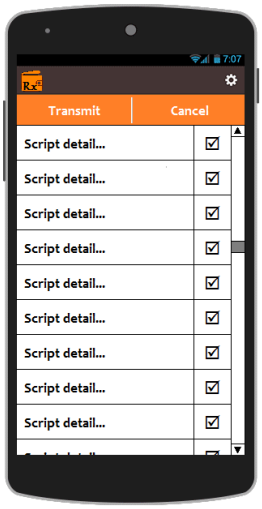

Figure 8: Script selection screen of the fictional mobile prescription transfer application

The available metadata of an electronic prescription in eTP contains (A) document Id, (b) document Type, (C) qualified Retrieval Key, (D) author, (E) originator, (F) originator Organisation and (G) creation time of the electronic prescription. Since, this information has little use in the process of a user selecting prescriptions to transfer to the electronic dispensing system, the mobile prescription transfer application will decrypt the prescription payload upon receiving the prescription from the electronic prescribing system and extract certain information such as medication name for cataloguing purpose. Both the prescription payload and DAK will then be encrypted once the necessary information is extracted. Although the decryption of the electronic prescription by the mobile prescription transfer application appears intrusive and violating security measures, this operation is perfectly acceptable according the governing specification ATS 4888.2-2013. Whilst ATS 4888.2-2013 strictly prohibits derivation of any *Cipher Key*, *Retrieval Key* or *DAK Holder Proof Key* from a DAK by any

unauthorised systems/users, it does not impose any restriction for authorised users. In this scenario, the decryption of the prescription payload by the electronic prescription transfer application is deemed acceptable as the possession of *Retrieval Key* acts as the bearer credential and grants the holder the right to access the electronic prescription associated with it. Nonetheless, the information to be extracted (i.e. the name of the medication) is information that is currently readily accessible on the paper prescriptions as well as on the prescription notifications of the current eTP system.

DISCUSSION

Despite the drastic change in the way in which prescriptions are transferred, the necessary changes to be made at the prescribing end (i.e. in Electronic Prescribing System - EPS) and the dispensing end (i.e. in Electronic Dispensing System - EDS) are expected to be minimal since both prescription transfer approaches, current eTP model using PES and proposed transfer model using patient's mobile smartphone, fundamentally utilize the same mechanism (i.e. DAK) for ensuring the security of the electronic prescriptions. This drastic change in the transfer process is evident in figure 1 and figure 5 as they portray the obvious differences in the way in which prescriptions are transferred. However, despite the controversial change in the transfer process the encryption and decryption of the prescriptions are done in the same way and how little it has changed can be evident in the figure 2 and figure 6. The impact by the change introduced is isolated to the transfer process alone and the proposed approach doesn't introduce any new idea or concept in any other part of the prescribing process thus limiting the required changes in other parts to be minimal.

In the current approach, DAK being a long series of random alphanumeric characters makes it hard to have knowledge about it unless it is explicitly disclosed to. Therefore, having knowledge of the DAK grants the knowledge holder the right to retrieve the prescription. However, DAK printed on the prescription notification can be scanned by most of the barcode scanner application and there is no other security measures once someone got a hold onto the DAK. In addition, there are cases of prescriptions being forged by simply scanning and reprinting it with decent quality scanning and printing equipment. In the proposed approach, the prescription is literally under the patient's full control and it will take more than just a DAK alone to get it. Therefore, the chances of a prescription being forged in the proposed approach is fairly slim. The proposed approach also make use of NFC's design for close proximity communication as an additional security feature since it makes unauthorised sniffing or intercepting the prescription information a lot harder than scanning a barcode from a printed paper.

At present, information such as prescription expiration and number of repeats left are only available to the dispensing party and may not be advised to the patient. These information will practically be in the patient's hand with the proposed approach. More importantly, it is now possible to implement the alert feature for drug allergy and harmful doses as part of the mobile electronic prescription transfer application; the feature which have been disabled in electronic prescribing systems some time ago due to having unfavourable effects on workflow, communications and prescribing process as a whole. The current approach requires the Internet connectivity for downloading the prescription from PES prior to dispensing and for submitting the dispense record after dispensing the medication. Therefore, the dispensing process cannot take place in absence of the Internet connectivity. With the proposed approach, the prescription will be downloaded from the patient's mobile device prior to dispensing and the dispense record will be uploaded back to the mobile device for necessary update after dispensing the medication. Subsequently, updating of National Prescription and Dispense Repository (NPDR) and Pharmaceutical Benefits Scheme (PBS) claiming processes will continue to function in the same way. In the absence of the Internet connectivity, the proposed approach will continue to function and allows the EDS to retain those transactions for batch submission at later time if there were no Internet connectivity at the time of dispense.

CONCLUSION

The proposed mobile electronic prescription transfer approach is a cheaper alternative, with comparable security measures, to those of the current approach using a PES. This new approach eliminates the associated on-going costs and puts the patient in control of their personal and sensitive information without having negative impacts on the public health initiatives and government recorded data such as National Prescription and Dispense Repository (NPDR). This approach enables patients to take more responsibility for their health and having them in control of their sensitive information allows them to prevent undesirable secondary use of that information by third parties. It also reduces the complexity of, and removes the dependency on, the major supporting infrastructure and Internet connectivity, therefore functioning just as effectively in remote locations with poor or non-existent connectivity. However, it is not a flawless solution. Due to the disconnected nature, it cannot perform certain features currently supported by PES services such as prescription requests and cancellation of

prescriptions. On the other hand, this proposed alternative also opens up opportunities to incorporate certain useful features such as prescription expiration alert and last repeat alert, functionalities that currently reside with dispensing systems, but are not communicated to a patient unless a prescription is dispensed. More importantly, the ability to implement the alert features for drug allergy and harmful doses as part of the mobile electronic prescription transfer application significantly improves the patient safety and benefits all parties involved in the prescribing process.

REFERENCES

Coskun, V., Ok, K., & Ozdenizci, B. (2013). *Professional NFC Application Development for Android*. Wrox.

ECMA International (2013). *ECMA-340: Near Field Communication - Interface and Protocol (NFCIP-1).* Retrieved from http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-340.pdf

Henderson, J., Pollack, A., Gordon, J., & Miller, G. (2014). Technology in practice – GP computer use by age. Australian Family Physician, 43 (12), 831-831

Htat, K. K., Williams, P. A. H., & McCauley, V. (2015). The Hare and the Hortoise [*sic*]: The Potential Versus the Reality of eTP Implementation. In *Proceedings of the 23rd Australian national Health Informatics Conference 2015* (pp. 114-120). Brisbane, Australia.

McDonald, K. (2015). eScripts continue to grow as eRx racks up a billion. Retrieved September 28, 2015, from PULSE+IT: http://www.pulseitmagazine.com.au/australian-ehealth/2596-escripts-continue-to-grow-as-erx-racks-up-a-billion

Smart Card Alliance (n.d.). NFC: Facts at a Glance. Retrieved from http://www.smartcardalliance.org/resources/pdf/NFC_Facts_at_a_Glance_060711.pdf

Standards Australia. (2013). *Electronic transfer of prescriptions Part 2: Platform independent (logical) services model to support electronic transfer of prescriptions* (ATS 4888.2-2013). Retrieved from http://www.e-health.standards.org.au/Home/Publications.aspx