12-4-2013

A Rapidly Moving Target: Conformance with E-Health Standards for Mobile Computing

Patricia A.H. Williams
Edith Cowan University, trish.williams@ecu.edu.au

Vincent B. McCauley
Medical Software Industry Association, vincem@mccauleysoftware.com

DOI: 10.4225/75/57981c3131b41
2nd Australian eHealth Informatics and Security Conference, held on the 2nd-4th December, 2013 at Edith Cowan University, Perth, Western Australia

A RAPIDLY MOVING TARGET: CONFORMANCE WITH E-HEALTH STANDARDS FOR MOBILE COMPUTING

Patricia A H Williams[1] Vincent B McCauley[2,]
[1]eHealth Research Group, School of Computer and Security Science, Security Research Institute,
Edith Cowan University, Perth, Australia
[2]Medical Software Industry Association
[1]trish.williams@ecu.edu.au, [2]vincem@mccauleysoftware.com

Abstract
The rapid adoption and evolution of mobile applications in health is posing significant challenges in terms of standards development, standards adoption, patient safety, and patient privacy. This is a complex continuum to navigate. There are many competing demands from the standards development process, to the use by clinicians and patients. In between there are compliance and conformance measures to be defined to ensure patient safety, effective use with integration into clinical workflow, and the protection of data and patient privacy involved in data collection and exchange. The result is a composite and intricate mixture of stakeholders, legislation, and policy together with national and individual perspectives. The challenges for standards development are numerous and include the cross over from traditional medical devices and mobile devices with apps, as well as harmonisation for consistent semantic terminology, and the diverse range of standards required in mobile health solutions. These issues affect the ability of conformance and compliance to be undertaken. Additionally, the need for interoperability in development of safe and secure mHealth software whilst being mindful of the implications for patient safety is vital. Conformance and compliance to established international standards is the first and, at present, the only step in meeting the mobile health challenges.

Keywords
Health Informatics, Standards, mHealth, Mobile Health, Health Software, Patient Safety, Information Security.

INTRODUCTION

The mobile ehealth marketplace is already significant and growing at a rapid rate. In 2013, the mHealth market globally was valued at $6.6 billion and projections place this to rise to $20b-$26b by 2018 which is an annual growth rate of more than 25% (PWC, 2012; RnRMarketResearch, 2013; Terry, 2013). In 2012 there were 44 million health app downloads with some 13,000 iPhone consumer health apps ("Number of Health Apps Rising, but Download Rates Remain Low", 2012) and global revenue of mobile health apps of US$1.3 billion. “There are already roughly 100,000 health applications available in major app stores, and the top 10 mobile health applications generate up to 4 million free and 300,000 paid daily downloads. Consumer adoption of mobile health apps will proceed apace” (Workman, 2013). This unprecedented growth raises questions on how much legislation and standardisation should be exerted to control this growth, or should policy makers rely on organic growth and self-regulation in the mobile industry.

This mobile ehealth application and services environment is collectively referred to as mHealth. Formally, “Mobile Health (mHealth) is the use of communication between mobile devices and to other devices for the purpose of Healthcare and patient well-being” (HL7, 2013).There are two distinct emergent areas of application for mobile health: consumer based including applications for wellness, disease prevention information, diagnosis through interactive consultation, treatment compliance and reminders, and monitoring vital signs and alerts ; and those that aim to strengthen the healthcare system by improving efficiency of service delivery such as emergency response and vital sign tracking, healthcare surveillance data collection, clinical decision support and clinical information, and healthcare administration reminders (PWC, 2012).

Given the exceptional escalation in both devices and applications, and the integration with medical devices, there is a need for broad reference architectures for mobile health that can define the capabilities and support structures required for reliable and secure mobile services in health. Of concern is that in 2012, 60% of confidentiality and security breaches reported to the US Department of Health and Human Services as a mandatory requirement of the Health Insurance Portability and Accountability Act (HIPAA) regulation, were from loss or theft of mobile and portable devices (Kruger & Anschutz, 2013). This issue becomes increasingly complex not only because of the proliferation of devices and ease of development of mobile applications, but because of the additional regulation that applies when dealing with health and medical information (McMahon, 2013). The mHealth market is highly fragmented (GSMA, 2011; RnRMarketResearch, 2013). This poses

significant challenges when solutions are attempting to address transparent interoperability, security in data transfer, availability of use, as well as the delivery of mHealth services. Added to this is the complexity and misunderstanding that surrounds the interpretation of data protection in general in the healthcare environment (Williams, 2013). The concern over poor governance processes in relation to information security, which underlie accountability at an organisational level, will only become more intricate (Strobl, Cave, & Walley, 2000).

E-health mobile applications for clinical providers are relatively immature. However it is clear that the key to adoption in clinical practice is leveraging existing ehealth standards to support effective communication and seamless exchange of health information on mobile platforms. The lines between traditionally defined medical devices, which now have both embedded and stand-alone software, and mobile devices using software that turns the device effectively into a 'medical device' are becoming increasingly blurred and difficult to discern. This poses significant problems because medical devices are strictly regulated and untangling this crossover to develop international standards is becoming increasingly difficult. In conjunction with this it is inevitable there will be a need for mobile specific ehealth standards, which are already emerging, as are the associated regulatory environments (Laakko, Leppänen, Lähteenmäki, & Nummiaho, 2008).

With these multiple concerns highlighted, this paper provides a discourse on the current work and emerging challenges, nationally and internationally, in regards to standards development for mobile health software. This includes the impact and issues with standards adoption and the associated conformance and compliance problems. The resultant impact on patient safety and the increasing risk to patient privacy and security of health information is discussed.

THE UNDERPINNING PROBLEMS

There is an increasingly blurred delineation between ehealth software and medical devices particularly in the mobile marketplace. This is, in part, due to the global availability of sensor technologies such as global positioning systems (GPS), touch screens, cameras and audio/video. These in turn are further enhanced by the availability of cheap simply interfaced add-ons to mobile phones that enable sophisticated sound acquisition processing (the i-stethoscope) and physiological trace acquisition and analysis such as the new iPhone back cover to acquire a single lead electrocardiograph (ECG) and software to perform trace analysis (D'Angelo, Schneider, Neugebauer, & Lueth, 2011). In conjunction with software to manage patient records and acquire patient data, mobile devices are both medical devices and platforms for ehealth software. Hence, they present significant policy challenges to regulators and require new ways of looking at clinical best practice to embrace mHealth.

There is no disagreement that digital health is being driven by the convergence of technology, specifically Smartphone technology, wireless communications and the decreasing costs of monitoring and medical data acquisition devices. The potential to reduce ongoing costs of healthcare delivery by providing improved and alternative methods for information access is attractive (Burrill, 2012). Clearly, early detection and intervention of disease as well as reducing post hospitalisation re-admittance are significant benefits to the health system as well as individual patients. This prevention and promoting healthier behaviour is a key factor in the majority of the health and wellness mobile applications accessible for Smartphone technology.

The challenges lie in the integration of standards-based health solutions, including mobile applications, so that they actually benefit the patient in a cohesive and holistic manner. The Continua Alliance, an alliance of 230 organisations working towards developing an ecosystem for personal health solutions, sees mobility as a key factor. However, there are three significant barriers which present a minefield for this development. These are a lack of maturity in the mobile environment which means that creating stable models for development are problematic; some standards and profiles for interoperability are not freely available or yet to be developed; and the regulatory environment is both confusing and also suffering from a lack of maturity (Cnossen, Jorgensen, Krishna, McClellan, & Rogers, 2010). Despite the development of new 'shrinking' networks such the Personal Area Network (PAN) and the newly defined Body Area Network (BAN) (Martí, Delgado, & Perramon, 2004; Penders et al., 2009), it is not the technology that is hindering the progression of mobile solutions, rather the difficulty in integrating the information transfer seamlessly and ensuring semantic interoperability.

To support effective communication, mobile devices must support existing standards for information exchange as they provide for the seamless and secure exchange of health information, which includes a standards-based approach, openly interoperable systems and devices, and cooperation between healthcare providers and mobile development and devices (GSMA, 2011). As part of its social responsibility, government must attempt to ensure public safety and healthcare is a particularly sensitive area to address. Where new initiatives that are not as yet

unequivocally proven to be beneficial and safe, governments step in to regulate use and therefore growth. The US Food and Drug Administration (FDA) have not taken a laissez-faire attitude to mHealth and have put in place new guidance rulings for mobile applications. This guidance redefines a mobile device as a medical device, and therefore under stricter control, in certain circumstances. The FDA oversight of mobile medical apps states that medical device regulation applies where the mobile app (FDA, 2013):

- Is intended to be used as an accessory to a regulated medical device. E.g. apps that allow health professional to make specific diagnosis by viewing a medical image from a picture archiving and communication system (PACS) on Smartphone or mobile tablet; or
- Transform a mobile platform into a regulated medical device – e.g. app that turns a Smartphone into an electrocardiography (ECG) machine to detect abnormal health rhythms or determining if a patient is a experiencing a heart attack.

This approach is based on functionality, is platform agnostic, and is related to the preservation of patient safety under conditions where the application does not function as intended. The FDA stipulates that this guidance is nonbinding and not legally enforceable; however, they may be affected by regulatory requirements where the FDA has cited any link. Indeed, it is the interpretations of the regulations that are cited in lawsuits (MDDI, 2013). Whilst Australia has not yet adopted a legislative approach, it is taking steps to provide guidelines on application development and personal privacy (Office of the Australian Information Commissioner, 2013). This guide is to assist mobile app developers ensure they comply with Australian privacy legislation as the Privacy Act regulates the way in which 'personal information' is handled. This includes

- Photographs;
- Internet Protocol (IP) addresses, Unique Device Identifiers (UDIDs) and other unique identifiers in specific circumstances;
- contact lists, which reveal details about the contacts themselves and also a user's social connections;
- voice print and facial recognition biometrics, because they collect characteristics that make an individual's voice or face unique; and
- location information, because it can reveal user activity patterns and habits.(Office of the Australian Information Commissioner, 2013).

The exponential development and use of computer and software products as medical devices together with the varied and broad range of products that became available meant that trying to regulate or control the mobile environment was a challenging task. Hence a standards based approach is relied upon to provide both the potential benefits realisation of interoperability as well as promoting patient safety through conformance. Unlike the USA, this approach promotes best practice against privacy rather than adopting a regulatory approach.

In order to understand the issues in standards conformance and compliance, it is first necessary to appreciate the complexities around standards development and adoption in the mobile space.

Standards development complexities

For successful development of mHealth, agreement on interoperability needs to be established. What interoperability means is that there must be a common understanding of the data elements, structures and terminology used in the mobile and health IT space. This is inclusive of functional consistency with common functions and procedures, and semantic commonality. Such interoperability requires standards to be effective (Hammond, 2005).

mHealth is a broad field and no single standards organisation encompasses the entire field. However, supporting and enabling development are international standards organisations that are at the forefront of interoperable healthcare mobile standards development. These include Integrating the Healthcare Enterprise (IHE), Health Level 7 (HL7) and International Organisation for Standardisation (ISO). IHE and HL7 in particular are the leading standards developers for healthcare information interoperability, messaging and architecture.

As the following discussion highlights, there is considerable amalgamation and interpretation of use of these standards for the ehealth mobile environment. In addition, the fragmented nature of standards development for mHealth is demonstrated with each Standards Development Organisation (SDO) focused on a different piece of the mHealth puzzle.

Integrating the Health Enterprise (IHE)

The network stack available on most mobile devices does not support higher level internet protocols such as Simple Object Access Protocol (SOAP). The development of RESTful (representational state transfer) services which requires only HTTP protocol availability has enabled deployment of service oriented architecture (SOA) standards based software to mobile platforms.

In August, 2012 IHE published for trial use, the Mobile access to Health Documents (MHD) profile which specifies a RESTful service to enable simplified access to a Cross Enterprise Document Sharing (XDS) infrastructure, as well as other ehealth repositories (IHE ITI Technical Committee, 2013). Designed specifically to support simplified interactions, consistent with a single policy domain use, in Cross-Enterprise sharing it includes support for security, privacy and interoperability. It defines a simple HTTP interface to an XDS environment by defining transactions to submit a new document and metadata from the mobile device to a document receiver; get the metadata for an identified document; find document entries containing metadata based on query parameters; and retrieve a copy of a specific document. This provides a profile for constrained environments such as mobile devices which allows mobile devices to access the many XDS ehealth data repositories as well as other data repositories that support a minimal service interface (IHE ITI Technical Committee, 2013). This puzzle piece addresses the request and transfer aspects specifically for mHealth data transfer.

Health Level 7 (HL7)

HL7 is arguably the preeminent contributor to date of all the healthcare standards development organisations. Examples of development of mobile related integration began as early as 2006 with device to electronic health record interoperability (De Toledo, Lalinde, del Pozo, Thurber, & Jimenez-Fernandez, 2006). In 2008, an HL7/Clinical Document Architecture (CDA) framework was demonstrated using a mobile tele-ECG use-case (Laakko, et al., 2008). A further example is the implementation and integration of key elements of HL7 and SNOMED (Systematized Nomenclature of Medicine) for mobile application, which have been addressed since (Benson, 2012). HL7 formally authorised the Mobile Health Working Group in January 2012, and it is currently focussed on the new Fast Health Interoperability Resources (FHIR) RESTful service based standard for simplified interchange of HL7 artefacts. This work has been enthusiastically adopted by implementers and due to its architecture is being deployed on mobile devices where it provides a capability of integrating HL7 messaging and existing document paradigms.

International Organization for Standardization (ISO)

ISO TC215, the International Organization for Standardization's (ISO) Technical Committee (TC) on health informatics, has been providing standards for mobile medical devices for some time as part of the *ISO/IEEE11073 'Health informatics -- Personal health device communication' family of standards.* These include a specialised 'Bluetooth for Health' standard, which incorporates enhanced security, as well as sensor data acquisition standards. These have been leveraged by the Continua Alliance (Cnossen, et al., 2010) to develop a range of mobile devices and ehealth platforms that communicate securely using the IHE XDR (Cross-Enterprise document retrieval) profile.

However, what is important to be aware of is the increasing complexity and overlap that mobile health is provoking. The following is an example of the difficulties now emerging in developing these standards. A joint working group (JWG7) established between IEC 62A (International Electrotechnical Committee 62A Common aspects of electrical equipment used in medical practice) and ISO TC215 has published the initial standard that sets basic requirements for setup and management of safe medical networks incorporating medical devices including mobile devices – *ISO/IEC 62A 80001 Application of risk management to information technology (IT) networks incorporating medical devices*. A series of technical reports and related standards is in the process of being published to facilitate implementation of this standard. In addition, JWG7 is working on a standard for the requirements to enable safety in ehealth software which will also be applicable to mobile devices – *ISO/IEC 82304-1: Health Software – Part 1: General requirements for product safety*. This standard has arisen in response to the need for a standard that extends *ISO IEC 62304:2006 Medical device software -- Software life cycle processes*, which itself is based on *ISO/IEC 12207:2008 Systems and software engineering -- Software life cycle processes*. One of the main issues in the harmonisation of these standards is the number of levels of classification of risk.

IEC 62304 was originally published 2006, and it assumes that the software has overall system requirements – i.e. embedded software within a medical device or that other system requirements are necessary. In comparison,

ISO/IEC 82304 looks at software without the overarching systems (medical device) in place. To increase the complexity in the development of the co-existing standards, issues that reflect the evolution of the medical environment to a more health oriented environment together with the rapid development in technology (i.e. mobile) have emerged in term of terminology as well as content. For instance, the term 'manufacture' is used exclusively in standards associated with medical devices rather than 'develop' or 'produce' as in common use in regards to software development. These issues alone are causing significant delays in development and harmonisation of the standards.

Notably, the classification for patient safety is a vital emerging factor for health software safety which was originally based upon the anticipated severity of harm, but is now moving to assessment based on more traditional security reasoning on risk, where likelihood of occurrence has been added. It is also scalable to health software which does not lead to severe outcomes, for instance mobile apps. For an overview of the standards that apply in this area, refer to *ISO TR 17791 Health informatics -- Guidance on standards for enabling safety in health software*.

Legacy, in terms of health software, is also a significant concern in terms of patient safety. Mobile apps can be added to this list given their uncontrolled development, and these can be termed legacy systems where they were developed in the absence of any requirements to meet these standards.

In addition to the mHealth standards, a number of underlying supporting technical standards including short range wireless such as Bluetooth and Zigbee (used in PAN and BAN mHealth architectures) have been adopted. As listed below, these underpin and strengthen the development in mHealth:

- ISO/TR 21730:2007 Health informatics -- Use of mobile wireless communication and computing technology in healthcare facilities -- Recommendations for electromagnetic compatibility (management of unintentional electromagnetic interference) with medical devices
- ISO/TR 27809:2007 Health informatics -- Measures for ensuring patient safety of health software
- ISO / IEC/CD 82304-1Healthcare software systems -- Part 1: General requirements (under development) looking at the safety of health software.
- ISO/DTR 17522 Health informatics -- Provisions for Health Applications on Mobile/Smart Devices, currently under development, researches existing mHealth architectures and classifies them into three categories: Integrating the Healthcare Enterprise (IRE) Mobile access to Health Documents (MHD); Mobile Electronic Medical Record (EMR); and Mobile Medical Apps.

In summary, both the classification for patient safety, and conformance to standards and directives, are key issues for health software particularly for mHealth.

ISSUES IN STANDARDS ADOPTION

Unfortunately there is no overarching map of what standards are needed in healthcare. There is no 'grand plan'. Currently standards development is driven by implementation needs and by specific interest of groups or individuals. It is clear that the issues identified in the development of standards have an impact on the adoption, conformance and compliance in such a diverse range of standards. The fragmentation of development across organisations, each looking at different puzzle pieces; ensuring interoperability between standards that are used together in an end-to-end mobile health solution; and the difficulties in harmonisation and terminology inevitably impact compliance. Further, there are more issues relating to conformance and compliance which crosses over from health software to mobile applications and medical devices. These issues relate to the approach to conformance and the difference in objectives between one the one hand governments in overseeing governance and safety, and on the other hand industry who develop applications and software. Whilst there are essential challenges of conformance to standards there are also major benefits. Part of the contention is in the methods and types of assessments and what should be enforced, what should be adopted as best practice, and what form accreditation should take.

Government versus industry objectives

The ehealth mobile market will challenge current governance arrangements and bring into starker contrast the different requirements of government and industry. Government is focussed on political drivers and relatively short times frames in an environment of frequent personnel changes and the need for flexible outcomes. By

contrast, industry works best with medium to long term planning, and fixed scope developments that have a sustainable business case.

Conformance, accreditation and certification

To ensure software products and systems are safe and meet quality parameters, conformance, accreditation and certification is used as measures against standards.

- Conformance involves testing similarity of an implementation to a standard/specification. Conformance to the published standards is required to establish that the software or product meets that standard. Ii is defined as testing to see if an implementation dependably meets the requirements specified in a standard. This testing must be to the criteria specified as conformance points specified in the standard, and may include functionality, interoperability, performance and behaviour. Conformance assessment refers to a complete testing process and is an internationally standardised term (AS/NZ ISO 17000) incorporating the concepts of compliance assessment, conformance assessment and product certification. There are four methods for assessment that are used in conformance in health.

    1. First-Party Assessment. This is essentially a self-assessment 'supplier assessment' and is known as a supplier's declaration of conformity.

    2. Observed First-Party Assessment. This is where self assessment is undertaken with observation by an independent third party. This mostly occurs at a Connectathon, where developers with expertise in the underlying architecture, are present. For instance the IHE and FHIR Connectathons.

    3. Second-Party Assessment. This method also referred to as 'Customer Assessment', invites a potential customer of the supplier to verify that the product it is offering conforms to relevant standards/specifications.

    4. Third-Party Assessment. This occurs where an independent assessor, for instance a certification body, performs the conformity assessment.

- Accreditation is the formal recognition that an organisation or a person is competent to carry out specific tasks. Accreditation is a specific form of certification, referring to the certification of bodies approved to perform conformity assessment.

- Certification is the authoritative act of assessing compliance/conformance. It is an independent attestation that software meets the requirements of a set of assessment schemes. Certification provides enduring guarantee of conformity and must be performed by a third-party organisation that has been accredited by a recognised accreditation body (eHealth CCA Governance Group, n.d.).

Conformance is critical if we are serious about semantic interoperability. The major issue is in balancing sufficient conformance to enable best practice and ensure safety, whilst still allowing flexibility in implementation and not stifling innovation (Slabodkin, 2013). Further, it should be proactive and not as a penalty or limiting regime.

Another issue is that of the testing methodologies that are most appropriate. Whilst static implementation testing using specialised IT test laboratories is possible these need specific e-health and mobile health knowledge. Whilst some exist such as the US Certification Commission for Health Information Technology (CCHIT) and Australian Healthcare Messaging Laboratory (AHML), they cannot cater in the current environment for mobile health applications. Further, for conformance to work, it requires that all standards clearly define the conformance points or policy developed conformance requirements. An alternative to this is Interoperability testing using events such as the IHE Connectathon. Lastly, site specific installation testing is also an option and is the role for certification.

The benefits of conformance and certification can be realised in safe and quality health software with consistent documentation and reuse of specifications possible, supported by independent and objective evaluation. It also provides lower integration costs and facilitates plug and play approaches, as well as avoiding vendor lock-in. To date the conformance of health software to its underlying standards and specification, particularly in Australia, has been to ensure interoperability rather than software specific criteria focussed on software quality and safety. Unfortunately the present composition of the mobile health solutions means a large number of vendors are part

of each solution, each with different platforms, systems and standards usage. Hence, whilst conformance is a step in the right direction it is of itself not the solution to ensuring patient safety.

ISSUES FOR PATIENT SAFETY

Clearly conformance is required to ensure patient safety of software in as far as standards can support this objective. Ensuring software compatibility and semantic interoperability is a necessity. However, this is not the entire solution. Mobile health is a specialised example of a health information system, and as such will suffer from the same vulnerabilities as other health information systems from a patient safety perspective. Without a doubt, the definition of patient safety extends to the issues of privacy and security as the impact of these can affect patient safety and well being.

Unfortunately, research shows that the issue of clinical safety and health information systems mainly consists of random initiatives world-wide. This means there are significant gaps in the mechanisms for safety assurance associated with the full range of healthcare information systems (Magrabi et al., 2013) including those involved in mHealth activities. Given the diversity in mHealth it is not surprising that assessing patient safety is problematic. What is evident is that mHealth including networked medical devices has benefits and drawbacks. They potentially will be both transformational and disruptive in healthcare delivery whilst at the same time may expose serious patent safety concerns. "Among the unintended consequences of health care's digitization and increased networked connectivity are the risks of being hacked, being infected with malware, and being vulnerable to unauthorized access and security" (Jones & Coughlin, 2013).

Other challenges exist in terms of identifying a patient that is using a mobile device or is the healthcare subject of a mobile device application, especially in jurisdictions that do not have a unique patient identifier, although the latter is by no means a panacea. In addition, ensuring safe consistent data display across heterogeneous mobile devices using applications that are not mobile specific can be difficult and may pose safety hazards where critical data is not displayed or is formatted incorrectly.

This is clearly an area that needs urgent attention and in Australia there are several groups beginning to address this including the eHealth Industry Clinical Safety and Security Committee, and the University of New South Wales - Centre for Health Systems and Safety Research.

The increasing risk to patient privacy and security

Mobile ehealth presents some unique challenges. Mobile devices are generally operated in physically insecure environments with less secure network technologies such as Wi-Fi and Bluetooth. In addition, security policy frameworks and governance of locally held data is either absent or incomplete. A lack of support for common tokens such as USB or smart card, leads to a reliance on less secure software only protection. This is coupled with an environment that is less mature in respect to malware defences against Trojans and viruses. In addition, the challenges of diverse platforms and development environments that exist in the mobile context make the need for a standards based approach even greater. A standards based approach will help realise the benefits of safe, high quality, well documented software that can be reused and integrated easily and minimise vendor lock-in. Accordingly, a strong standards base can provide a platform for rapid, relatively low cost innovation.

Security presents a gamut of issues that need addressing in the use of mobile devices in the healthcare setting. Common mobile devices have "hidden" data stores and logs which can be a source of compromise of patient/provider confidentiality. Support for standard public key infrastructure (PKI) certificates routinely used for ehealth encryption and authentication, and their associated software libraries is not generally available. It is by and large considered that 256 bit encryption should be a requirement in the mobile environment, but there are restrictions on export of such applications in some jurisdictions. Hence, local data storage, even if encrypted, may be at risk. In addition, the commonly used Wi-Fi and Bluetooth wireless communication protocols have well described vulnerabilities that need to be taken into account when using mobile devices "in the wild". However, implementation of sophisticated encryption algorithms and secure network protocols, such as virtual private networks (VPN), lead to complexity, slow performance and reduced battery life that with current devices may discourage use.

To date the standards have focussed on the implementation end of the ehealth informatics spectrum, therefore trusted interoperability may present problems, in the case of additional or bolt-on software, where agreement between software vendors and use of application programming interfaces (API), creating trusted and safe interoperability, may be absent (McCauley & Williams, 2011). Yet, it is emerging that urgent attention is required at the opposite end where development of software and applications begins.

CONCLUSION

Whilst implementation in a technical sense is well understood, one of the rapidly evolving barriers is in the effective use of the resultant information, and how this is both catered for in workflow and what its impact on workflow will be. This could be a significant barrier to moving past simple health and wellness mHealth to more clinically based applications. The future is exciting for personal mHealth. The development of technology such as body powered miniaturised sensor nodes, replacing existing medical devices, opens up a whole new world of opportunity for mHealth innovation. The integration and linkage of sensors and monitoring devices via mobile telephony direct to healthcare providers when it is needed is a huge step forward for preventative health. Perhaps given the complexity of interoperability across multiple platforms and devices, together with the integration of data into efficacious resources to affect clinical decision support, mobile health gateways will emerge to facilitate connection and transfer from mobile networks to existing healthcare information systems. Yet, all this will need standardisation, control and governance to ensure efficacy and patient safety in the design, implementation and use.

This paper highlights, not only the numerous facets that need interoperability in development of safe and secure mHealth solutions, but the complex nature of integrating these with effective deployment. The crossover from medical devices to mobile devices and software is increasingly complex. As yet, it is clear this confusion is in its infancy in regards to being sorted out, yet governments are reacting to the potential effect already with regulation of mobile applications. The mHealth market will eventually condense its development in the same way that the banking industry realised it would decrease costs whilst increasing customer satisfaction by working together to allow all automatic teller machines to accept each other's cards. What is evident though is that until the initial waves of development and adoption (and enthusiasm) for mHealth settles down and matures, the mHealth environment will abound with new and exciting innovations that unfortunately cannot be widely harnessed.

Ultimately the long term adoption of mobile applications will depend on ability of the application to deliver what is required and when it is required. Applications that do not follow the principles of a 'killer app' in not overwhelming a device with unnecessary data, only delivering the most important information automatically and at an acceptable receiving rate, will probably not last long in the marketplace (Baker, 2013).

REFERENCES

Baker, P. (2013). Finding the killer app. *Optimizing field services with mobility,* (June, 2013), 5, 13. Retrieved from <mobilefieldservices_0.pdf>

Benson, T. (2012). *Principles of health interoperability HL7 and SNOMED*: Springer.

Burrill, G. S. (2012). Digital health investment opportunities abound, but standouts deliver disruptive change. *Journal of Commercial Biotechnology, 18*(1), 49+.

Cnossen, R., Jorgensen, B., Krishna, J., McClellan, C., & Rogers, R. (2010). Continua enables standards-based mobile personal health solutions. [Discussion]. *Telemedicine and e-Health, 16*(4), 393+.

D'Angelo, L. T., Schneider, M., Neugebauer, P., & Lueth, T. C. (2011, Aug. 30 2011-Sept. 3 2011). *A sensor network to iPhone interface separating continuous and sporadic processes in mobile telemedicine.* Paper presented at the Engineering in Medicine and Biology Society,EMBC, 2011 Annual International Conference of the IEEE.

De Toledo, P., Lalinde, W., del Pozo, F., Thurber, D., & Jimenez-Fernandez, S. (2006, Aug. 30 2006-Sept. 3 2006). *Interoperability of a Mobile Health Care Solution with Electronic Healthcare Record Systems.* Paper presented at the Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE.

eHealth CCA Governance Group. (n.d.). *CCA Glossary.* Retrieved 11 Nov, 2013, from http://ehealthcca.com.au/about-cca/glossary.

FDA. (2013, 10/22/2013). *Mobile Medical Applications*. Retrieved 15 Nov, 2013, from http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/MobileMedicalApplications/default.htm.

GSMA. (2011). *A high level reference architecture for mobile health.* Retrieved from www.gsmaembeddedmobile.com.

Hammond, W. E. (2005). The Making And Adoption Of Health Data Standards. *Health Affairs, 24*(5), 1205-1213.

HL7. (2013, 8 August 2013). *Mobile Health Definition*. Retrieved 15 Nov, 2013, from http://wiki.hl7.org/index.php?title=MHWG_Definition,_Scope_and_Context.

IHE ITI Technical Committee. (2013). Mobile access to Health Documents (MHD) - Trial Implementation. *IHE IT Infrastructure Technical Framework Supplement*. Retrieved from http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_MHD.pdf.

Jones, R. L. & Coughlin, S. (2013). *Networked medical device cybersecurity and patient safety: Perspectives of health care information cybersecurity executives.* Retrieved from http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/Center%20for%20health%20solutions/us_chs_networkedmedicaldevice_091913.pdf.

Kruger, D., & Anschutz, T. (2013). a new approach to IT security. *Healthcare Financial Management, 67*(2), 104-106, 108.

Laakko, T., Leppänen, J., Lähteenmäki, J., & Nummiaho, A. (2008). Mobile Health and Wellness Application Framework *Methods of Information in Medicine, 47*(3), 217-222. doi: http://dx.doi.org/10.3414/ME9113.

Magrabi, F., Aarts, J., Nohr, C., Baker, M., Harrison, S., Pelayo, S, Coiera, E. (2013). A comparative review of patient safety initiatives for national health information technology. *International Journal of Medical Informatics, 82*(5), e139-e148.

Martí, R., Delgado, J., & Perramon, X. (2004). *Security specification and implementation for mobile e-health services*. Paper presented at the IEEE International Conference on e-Technology, e-Commerce and e-Service.

McCauley, V., & Williams, P. A. H. (2011). Trusted interoperability and the patient safety issues of parasitic health care software. In P. A. H. Williams (Ed.), *9th Australian Information Security Management Conference* (pp. 189-194). Perth: secau- Security Research Centre, Edith Cowan University.

McMahon, T. (2013, 2013 Feb 27). The smartphone will see you now. *Maclean's, 126,* 46.

MDDI. (2013). FDA Guidance on Wireless Devices: What You Need To Know. *Medical Device and Diagnostic Industry*. Retrieved from http://www.mddionline.com/article/fda-guidance-wireless-devices-what-you-need-know

Number of Health Apps Rising, but Download Rates Remain Low. (2012). Retrieved from http://www.ihealthbeat.org/articles/2012/7/17/number-of-health-apps-rising-but-download-rates-remain-low.aspx.

Office of the Australian Information Commissioner. (2013). *Mobile privacy: A better practice guide for mobile app developers consultation draft - April 2013*. Retrieved 11 Nov, 2013, from http://www.oaic.gov.au/privacy/privacy-engaging-with-you/previous-privacy-consultations/mobile-privacy-may-2013/mobile-privacy-a-better-practice-guide-for-mobile-app-developers-consultation-draft-april-2013.

Penders, J., Van de Molengraft, J., Brown, L., Grundlehner, B., Gyselinckx, B., & Van Hoof, C. (2009, 3-6 Sept. 2009). *Potential and challenges of body area networks for personal health.* Paper presented at the Engineering in Medicine and Biology Society, 2009. EMBC 2009. Annual International Conference of the IEEE.

PWC. (2012). *Touching lives through mobile health. Assessment of the global market opportunity*. Retrieved from http://www.pwc.in/assets/pdfs/telecom/gsma-pwc_mhealth_report.pdf.

RnRMarketResearch. (2013). *Mobile Health Apps Market: 80% Revenue of mHealth Market Dominated by Connected Medical Devices Segment Says a New Report*. Available at RnRMarketResearch.com *PRWeb*. Retrieved from http://www.prweb.com/releases/mhealth-apps-solutions/market-2018-forecasts/prweb11097745.htm.

Slabodkin, G. (2013). FDA's Bakul Patel: For mobile medical apps, patient safety first. *FierceMobile Healthcare*. Retrieved from http://www.fiercemobilehealthcare.com/story/fdas-bakul-patel-mobile-medical-apps-patient-safety-first/2013-05-23.

Strobl, J., Cave, E., & Walley, T. (2000). Data protection legislation: interpretation and barriers to research. *BMJ, 321*(7265), 890-892.

Terry, K. (2013). Mobile Health Market To Reach $26B By 2017. *Information Week* Retrieved from http://www.informationweek.com/mobile/mobile-health-market-to-reach-$26b-by-2017/d/d-id/1110964?

Williams, P. A. H. (2013). Information security governance: A risk assessment approach to health information systems protection. In E. J. S. Hovenga & H. Grain (Eds.), *Health Information Governance in a Digital Environment* (Vol. 193 Studies in Health Technology and Informatics, pp. 186-206). Amsterdam: IOS Press.

Workman, B. (2013). The Explosion In Health Apps, And How They're Disrupting The Gigantic, Lethargic Health Care Industry. *Business Insider*. Retrieved from http://www.businessinsider.com.au/mobile-will-disrupt-health-care-2013-9.