1-1-2010

Data security and information privacy for PDA accessible clinical-log for medical education in problem-based learning (PBL) approach

Rattiporn Luanrattana
University of Wollongong, rl631@uow.edu.au

Khin Than Win
University of Wollongong, win@uow.edu.au

John A. Fulcher
University of Wollongong, john@uow.edu.au

Recommended Citation

Luanrattana, Rattiporn; Win, Khin Than; and Fulcher, John A.: Data security and information privacy for PDA accessible clinical-log for medical education in problem-based learning (PBL) approach 2010, 979-984.
https://ro.uow.edu.au/infopapers/1733

Data security and information privacy for PDA accessible clinical-log for medical education in problem-based learning (PBL) approach

Abstract

Data security and information privacy are the important aspects to consider for the use of mobile technology for recording clinical experience and encounter in medical education. Objective: This study aims to address the qualitative findings of the appropriate data security and information privacy for PDA accessible clinical-log in problem-based learning (PBL) approach in medical education. Method: The semi-structured interviews were conducted with the medical faculty members, honorary clinical academics and medical education technology specialists. Results: Data security and information access plan were determined for managing clinical-log data. The results directed the guideline for the future development and implementation of clinical-log and other functionalities on PDAs. Conclusion: The findings provide the understanding of aspects, concerns and appropriate strategy to safeguard data security and information privacy of PDA accessible clinical-log.

Keywords

Data, security, information, privacy, for, PDA, accessible, clinical, log, for, medical, education, problem, based, learning, PBL, approach

Disciplines

Physical Sciences and Mathematics

Publication Details

Luanrattana, R., Win, K. Than. & Fulcher, J. (2010). Data security and information privacy for PDA accessible clinical-log for medical education in problem-based learning (PBL) approach. Proceedings 2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA) (pp. 979-984). Piscataway, New Jersey, USA: IEEE.

2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops

Data security and Information Privacy for PDA Accessible Clinical-Log for Medical Education in Problem-Based Learning (PBL) Approach

Rattiporn Luanrattana, Khin Than Win, John Fulcher
Faculty of Informatics, University of Wollongong, NSW, Australia, 2522
rattipornLnr@au.edu, {win, john}@uow.edu.au

Abstract— **Data security and information privacy are the important aspects to consider for the use of mobile technology for recording clinical experience and encounter in medical education. Objective: This study aims to address the qualitative findings of the appropriate data security and information privacy for PDA accessible clinical-log in problem-based learning (PBL) approach in medical education. Method: The semi-structured interviews were conducted with the medical faculty members, honorary clinical academics and medical education technology specialists. Results: Data security and information access plan were determined for managing clinical-log data. The results directed the guideline for the future development and implementation of clinical-log and other functionalities on PDAs. Conclusion: The findings provide the understanding of aspects, concerns and appropriate strategy to safeguard data security and information privacy of PDA accessible clinical-log.**

Keywords- e-learning, architectures for educational technology systems, data security and information privacy, computer-mediated communication, distributed learning environments, interactive learning environments, medical education, problem-based learning

I. Introduction

Data security and information privacy is one of the concerns in personal digital assistant (PDA) used in medical education and healthcare organization. The awareness of security and privacy has been emphasised for the incorporation of PDAs not only into healthcare organization but also medical education. Information access, storage and retrieval and the lose of data are the major concerns of PDA use in clinical practice [1]. The obvious concern is that the data is sensitive, and might be accessed and used by wrong people. Data security, therefore, is a significant aspect for the use of health information and PDA applications in healthcare organisation [2] as it demonstrates the confidentiality of data being kept in the systems [3]. Data security and information privacy issues are essential for wireless connectivity. It is necessary to ensure that data being recorded on PDAs are securely protected as there are risks of losing PDAs with private and confidential data.

This paper aims to address the possible data security and information privacy for PDA accessible clinical-log for problem-based learning (PBL)-medical curriculum at the Graduate School of Medicine (GSM), the University of Wollongong (UOW). The research questions are (i) what should be the appropriate information security techniques for PDA accessible clinical-log?; (ii) what aspects of information privacy should be considered in recording health information, clinical experiences and encounters regarding PDA accessible clinical-log? Therefore the literature reviews on the information security, security technology of mobile devices and information privacy of health information were conducted.

A. Information security, device security and data security techniques

Information security is a collection of policies and procedures to safeguard and maintain the integrity, availability and accessibility of information systems [4]. Security of information can be applied in term of hardware (device security) or software mechanisms (data security techniques).

Device security. PDA memory is easily removed, therefore a security policy is compulsory for data protection, for instance, data encryption and anti-virus protection with updated virus signatures [5]. Device management involves with a data synchronisation process. Data on PDAs will be merged with the management host. PDAs must be securely kept of all time [6].

Data security techniques. Data security procedures and techniques are applied to PDAs in order to safeguard information. Data security techniques are very much dependent on the requirements, interests and situation of each organisation. In terms of technical aspects, it is dependent on the availability and suitability of network resources, network infrastructure and other related factors. Possible data security techniques range from authentication with username and password, information access priority, data encryption, unobserved-ability, acknowledgement, services with special package and digital signatures, wireless communication security and wired equivalent privacy (WEP), biometrics identification, digital signatures, PKI, symmetric cryptographic algorithms, token-based two-factor authentication, data security for GPRS, GSM or 3G networks and backup procedures [4, 5]. However with current data security procedures, the majority of medical information is protected by username and password, which may possibly be insufficient in security aspect. Generally, data security also includes the data security for the mobile device and the network itself [7]. An *information access priority* should be applied to different groups of users. For backup information, it should be done centrally and

978-0-7695-4019-1/10 $26.00 © 2010 IEEE
DOI 10.1109/WAINA.2010.42

individually by central IT unit and individual user [8]. Further, data security also covers other aspects around computer viruses, worms and Trojan horses which may cause and spread from adware, spyware or cybercrime [9].

B. *Information privacy*

Information privacy is essential for healthcare providers and stakeholders to maintain and focus on the privacy of information and to protect the data from any unauthorised access [10]. Importantly, healthcare providers and users of health information need to abide by the privacy acts to ensure the patient's confidentiality [4, 10]. Health privacy legislations exist in various countries. For instance, the United States of America has the Health Insurance Portability and Accountability Act (HIPAA) that emphasises on health information. It is essential for all healthcare organisations and providers to follow this legislation. The ACT Health Records (Privacy and Access) Act 1997 emphasises 12 privacy principles. The Health Record Act 2001 and the Health Record and Information Privacy Act (HRIPA) 2002 are used in Victoria and NSW, respectively [4, 10]. The HRIPA comprises of 15 Health Privacy Principles (HPPs). Table I illustrates what NSW public and private sector must abide to the act when collecting, storing, using and disclosing health information.

TABLE I. FIFTEEN PRINCIPLES OF HPPS

Collection	1. *Lawful.* Health information should be corrected for lawful purposes. The collection of health information should be relevant to organisation's activities.
	2. *Relevant.* It is essential to ensure that the collection of health information does not breach individual.
	3. *Direct.* Only collect information directly from personal concerned.
	4. *Open.* It is essential to inform the person why health information needs to be collected, for what purposes and who will use the information.
Storage	5. *Secure.* Information must be securely kept and protected from unauthorised person.
Access and accuracy	6. *Transparent.* It is essential to inform the person about what health information to be stored and why it is being accessed and used.
	7. *Accessible.* The health information should be available for accessing without reasonable delay.
	8. *Correct.* Health information can be updated, corrected and modified if necessary.
	9. Accurate. Health information should be accurate and relevant before using.
Use	10. *Limited.* Health information should be used for its purposes, otherwise consent is needed.
Disclosure	11. *Limited.* Health information should be used for its purposes, otherwise consent is needed.
Identifiers and anonymity	12. *Not identified.* Unique identifiers must be used to identify people.
	13. *Anonymous.* Anonymity should be given to people as the option for receiving services.
Transfer and linkage	14. *Controlled.* Health information can be transferred outside NSW in accordance with HPP
	15. *Authorised.* People must express their consent to disclose their identifier for the purpose of the health records linkage system.

In regards to PDA use in healthcare and the medical professions is that PDAs are normally owned by individuals rather than particular units. Therefore transferring data, in particular patient information or electronic medical records (EMR) via PDAs could be uncontrollable in terms of patient privacy. It is possible that healthcare providers could limit access to health information or limit the ability to download and transfer patient information to PDAs or any computer [6]. On the other hand, the use of PDAs in medical education is more toward information accessing, communicating with peers, organising daily activities and recording information, for instance, clinical encounter. PDA accessible clinical-log is one of other PDA functionalities that may deal with sensitive information as such function is aim to facilitate students in recording clinical experiences and encounters. Therefore it is essential to identify the appropriate data security and information privacy.

II. METHOD

To answer the research questions, the semi-structure interview questions were formulated based on the literature reviews and scoping study. The interview questions were set out regarding data security and information privacy towards PDA accessible clinical-log and its use in a PBL-medical curriculum at the GSM. The *purposive sampling* by using criterion sampling strategy was used to select the participants. The in-depth interviews were conducted with 15 medical school stakeholders, including the GSM medical faculty members (n = 8), the educational technology team members (n = 4), and honorary clinical academics (n = 3) at Wollongong Hospital. The interviews were transcribed and analysed into themes and sub-themes using the `Nvivo` software package version 7.0. All interview questions were sent to the experts in medical education, educational technology and IT for their opinions. The interview questions were reviewed and revised for several rounds, based on the feedback received, to ensure that questions are valid and reliable for conducting the interviews. The *purposive sampling* by using criterion sampling strategy was used to select the participants.

III. RESULTS

Data security and information privacy is the most essential technical aspect for incorporating PDAs into the UOW PBL-medical curriculum. The findings on this aspect are directly relevant to data being recorded on a PDA accessible clinical-log and personal data being stored on PDAs. The findings regarding data security are particularly emphasised on (i) data security and security of PDA devices, (ii) information privacy based on the seven categories of 15 principles of HPPs, (iii) data disposal and (iv) professional conduct on practicing medicine (Table II).

Data security and security of PDA devices

The participants had a strong concern regarding (i) data security when dealing with patient information and (ii) the security of the PDA (Table II). The concern regarding data security is *identity fraud* and *security of PDAs* (as the device could be accessed by anyone in the case of losing a PDA). *Identity theft* or *identity fraud* includes the ability in accessing information on mobile devices by stealing devices, hacking data from database, etc. Moreover, PDA may contain a rich amount of personal information, which thieves or hackers can

TABLE II. OVERVIEW OF STUDY FINDINGS

Theme and sub-theme	Response from participants
A. Data security	*"…no need to physically move the technical interface from point A to point B."*
B. Information privacy	
1. Collection and use	*"…not the information that refers to individual. It is general information (e.g. age, gender), what the problem was, key learning features, the problems and learning outcomes, the student level of involvement and level of confidence."*
2. Storage:	
Where and how to store clinical-log information	*"…stored at the …secure room. …data is not to be kept in the students' PDA."*
Duration of data storage	*"…a minimum four years of their course. …to keep that data beyond the students' course… it may be helpful for research and comparing from cohort to cohort."*
3. Access and accuracy	
Data security and access plan	*"…a few people have an access…by username and password. …then managed by an educational technology team to ensure that system does not allow any security break…"*
Data accessibility and access authority	*"They shouldn't access towards the others rather than the potential person reflections (on clinical-log). If the students do … there will still be de-identified … no issue on breach of privacy."*
4. Disclosure	
Method of data disclosure	*"…at the highest level aggregation. … no identification of individual patients or students… no identification of the actual hospitals or clinical saying where the data came from."*
Accuracy of data disclosure	*"…any release of that information to anyone it contains no identified material. …If the data fields don't have any privacy data, there is no privacy data to hand-on the health information…"*
5. Identifiers and anonymity	*"…what confidentiality and how that is protected on all sort of levels whether verbal, written or electronic communication or whatever."*
6. Transfer and linkage	*"…no confidential information… they must be the students responsibility to distribute it."*
C. Data disposal	*"It would need to be done in a way that didn't leave anything behind."*
D. Professional conduct	*"…never viewing a confidential information about somebody else. …aware at every moment that you are dealing with personal and confidential information and respect that."*

use for unethical purposes, for instance, obtaining personal identifiable information to impersonate the owner of such information. In terms of clinical-log function, there are a number of data security procedures that can be applied, including access restrictions, access protection and access restriction on recording patient information. Besides these mechanisms, the security of data would rely on policy, regulations, guidelines, professional conduct and any health information and privacy act. It is also recommended that a reflection on clinical experiences with any written information or verbal communication must be done without specifying who the patient is.

The findings indicated that there are five aspects to be considered in order to secure PDA device and privacy of data. Theses aspects are (i) security of PDAs by not leaving PDA unattended; (ii) software mechanism by applying password protection for PDA device; (iii) data encryption techniques is recommend in case of storing or transmitting sensitive data; (iv) carefully use wireless connectivity as unauthorised person can access to PDAs via wireless connectivity; and (v) be careful on downloading software or resources as the software applications might be hidden with viruses or program that intend to steal users' personal information or password. However other software and hardware mechanisms could also be applied especially when transmitting data over the network, for instance, secure socket layer (SSL), WEB, device security, device management, etc. These data security mechanisms not only assist in protecting data from unauthorised access but also providing confidentiality and privacy of data. The findings are similar to the literature.

Information privacy

The patient information is the sensitive data. The primary purposes of using a clinical-log not only use for research and/or curriculum development but also for recording clinical encounters, including major clinical problems being found, and for physical diagnosis and then later discussion with the clinical preceptors. It is possible to use clinical-log data for discussing clinical cases, seeking feedback and using this for self-directed learning. Therefore the most important aspect besides using clinical-log data for medical study is to maintain patient privacy. The use of PDA accessible clinical-log with appropriate data security and privacy protection would ensure the security and privacy in recording, storing and accessing clinical-log data for all students and authorised users in the medical school. Knowing and understanding the primary concern with HRIPA would give students more confidence in practicing their medical profession. For information privacy of PDA accessible clinical-log data, seven aspects based on HPPs and HRIPA (Table I) should be considered when recording health information, clinical experiences and encounters.

Collection and use: What information can they access? - The information which the nominated faculty members and the educational technology specialists can access on clinical-log, namely clinical experiences, reflections on clinical experiences and learning outcomes without any patient identifiers (Table II). This information includes patient characteristics, clinical problems, adverse events, clinical experience rating, confidence rating and level of involvement. In comparison to other functionalities, which more involve referencing, information access and personal information management (PIM), these functions require less data security procedures as such. However these functions may also require access protection on the device, because it is possible that students may record their clinical experiences and personal reflections elsewhere on their PDAs. It is more secured for data if a protection scheme can be applied for PDAs.

Storage: Where and how to store clinical-log information - The majority of participants indicated that clinical-log data should be stored on the university's database server and maintained by the central IT unit rather than storing at the medical school (Table II) once students record their clinical experiences on PDA accessible clinical-logs. However the data is still supported and maintained by the GSM educational technology specialists. It has been stressed that clinical-log data should not be primarily stored on student PDAs or personal computers. Clinical-log data would be directly and automatically stored on the university's database. In this case, students record their clinical experiences on a given spreadsheet form, and their data will be stored on the university's database once students upload this spreadsheet file to their online clinical-log. Students are required to update and synchronise their clinical-log data to the university' server regularly [11].

Further, there are possible reasons why the clinical-log data must be stored on the university's server. The primary reason is for security purposes. Any authorised user can access the data once they are logged in and verified as an authorised user. Generally, such user will be given a different priority for accessing data. Secondly, it is for data management and security purposes. It provides the ease for the university's IT staff to maintain data in a centralised manner. Thirdly, it is secure as data is already protected in case students lose their PDAs or run out of battery. Finally, the medical faculty can easily access and monitor students' clinical-logs of experiences for assessment purpose via online access. Therefore both students and nominated medical faculty members would be able to access the same data source over time. This would provide speed, accuracy and reliability in information accessing. Furthermore, both students and the GSM can also maintain the interaction based on the recent update information, especially when students are away in the clinical placement elsewhere.

Duration of data storage: The participants' perceptions toward duration of storing clinical-log data in the database can be categorised into two major timeframes (Table II). Firstly, data can be stored on a database equivalent to the academic timeframes. Secondly, data can be kept for a longer period for future use. Generally, data being recorded on a clinical-log is generally used for academic purposes (for assessment tool, and the other is for future research, curriculum evaluation and for students future employment). Since clinical-log data is a record without identified information about patients, then there should be no issue regarding how long information should be stored on the databases, as long as the medical school can manage and maintain it.

In the case, where clinical-log data were health information then the timeframe to store this record would be based on the HRIPA. Therefore an appropriate timeframe could be applied which would depend on the purpose of using such clinical-log data in the future. A clinical-log is kept and used for reviewing students' progress during their clinical rotations and self-assessment during their medical study [11, 12]. To date, a little has been mentioned in the literature regarding having medical school store clinical-log data for future use. In addition, there are a number of medical schools that recommend students keep their own copy of clinical-log data for future employment [13, 14].

Access and accuracy: The findings reported the most to the least important aspects, these being (i) regarding data security and access plan, and (ii) data accessibility and access authority, respectively. The findings in each aspect were reported and discussed in the following sections.

- *Data security and access plan:* The GSM faculty have definite ideas regarding data security protection, namely that the access restrictions must be applied by providing authority only for students and several medical faculty members and educational technology specialists (Table II). These authorised people may be named or called differently by each medical school, for instance, tutor, preceptor, clerkship director, etc. However, the data security techniques and procedures are vary at each medical school, and would directly depend on what technique is applied to clinical-log function. Besides having limited access only for authorised persons, it is possible to apply relevant security techniques to enhance the security of PDAs in order to protect from interception or hackers. These security strategies include the use of passwords protection, data encryption, virus protection software, identification and frequent backing up of data.

- *Data accessibility and access authority:* The participants stressed that there is limited access to clinical-log data. Firstly, students can only access their own clinical-log. Secondly, the nominated faculty members can access certain levels of clinical-log data for assessment purposes. Finally, the educational technology specialists are able to gain access to clinical-log data for maintenance and support. Only a group of the medical faculty, clerkship director or tutor are able to access students' clinical-log data for assessment purposes [15, 16]. This authorised access allows them to monitor, investigate, comment and feedback on individual students' experiences during their clinical rotations. It is essential for students to maintain security of their clinical-logs by not letting any unauthorised person access, complete or fill-out any data.

Disclosure: data disclosure after graduation - There were a small number of the GSM faculty and the educational technology specialists with concerns about method of data disclosure after graduation and accuracy of the data disclosure process.

- *Method of data disclosure after graduation:* The participants had a similar perception regarding data disclosure (Table II), which can be categorised into three general opinions. Firstly, clinical-log data can be generally released by students without patient identifiers. (e.g. for future employment). Secondly, the medical school cannot disclose clinical-log information, which belongs to students without student consent. However, the medical school is allowed to use clinical-log information for research and evaluation of the medical curriculum. Finally, it is possible to disclose clinical-log data in a high-level report rather than a detail report for the Australian Medical Council or the medical school research and evaluation purposes. This type of research would contain no specific information about patient records.

The process of data disclosure essentially emphasises disclosing clinical-log information to anyone who is excluded from the process of medical education during 4-years of medical study. As a result, clinical-log data can be shared and discussed among peers, clinical preceptors and medical faculty members regarding the clinical experiences and encounters during the 4-years of medical study as part of the learning process. The findings are similar to the literature in that data can be disclosed only with the consent of an authorised person [6, 17]. Therefore, in order to disclose the data on students' clinical-logs, it is necessary to seek student consent.

- *Accuracy of data disclosure process:* Data accuracy from the medical school's perspective is to ensure that clinical-log data contains no patient's identifiable information (Table II); the data must be up-to-date before disclosed. This finding is similar to the literature regarding data disclosure by maintaining data privacy [18]. The accuracy of clinical-log data is ensured by students' clinical-log on PDAs being synchronised back to the central server within an appropriate timeframe.

Identifiers and anonymity: Privacy and anonymity of data - In this aspect, honorary clinical academics, the GSM faculty and educational technology specialists strongly support on maintaining privacy of patient information. Also, the others indicated that anonymity is essential when dealing with patients, particularly when recording patient characteristics and clinical problems encountered (Table II).

However, de-identified data can easily become identified information. For example, in recording a rare medical condition found in particular areas with particular patient characteristics, it would be easy to identify who the patient is. In such cases, it is important for students to make a judgment whether recording patient characteristics is compulsory for their self-assessment, whether it would be possible to omit some general characteristics by not recording them, but still reflect on their clinical experiences. Data security technology and programming techniques can be applied when developing and implementing the data entry interface of PDA accessible clinical-log particularly for a technical prevention. Without professional practice and conduct, this aspect would be an ideal solution. The findings on privacy and anonymity aspect generally agreed with the literature in that using a clinical-log to recorded clinical experiences and encounters is essentially similar to other medical schools, whether using paper-based or electronic-logs.

Transfer and linkage: Transferring information between two locations - It is the responsibility of students for their data and usage (Table II). However it is possible to attach the policy of using clinical-log information every time when data is transferred to a third-party elsewhere. This allows the third-party to be aware of what they can or cannot make use of with such clinical-log data. In case of transferring any sensitive data, data security approaches can be applied when transmitting data. This allows clinical-log data to have less privilege when being transferred to other users.

Data disposal

Three groups of participants had a similar perception towards (i) the method of disposing clinical-log information and (ii) how the school currently disposes clinical-log information. The data disposal includes both paper-based and electronic information on the clinical-log. Therefore in order to dispose of any unused clinical-log data, it is essential to ensure that data is thrown away in a safe bin or completely deleted from the computers or PDAs without resurrection (Table II). This finding differs slightly from the literature as students are free to edit, append or modify their clinical-log contents into multiple versions. As a result, the clinical-log function would not allow students to remove or delete any existing data in the log. From researcher's perspective, any unwanted data on the clinical-log must be disposed for information privacy purposes. Therefore data needs to be disposed of properly. Generally, clinical-log data is a valuable asset for both students and the medical school. On the other hand, in terms of storing clinical-log data on the university's database server over a long period for future use, secure data storage becomes an issue. The clinical-log data has to be stored in the systems for minimum 5-years before being disposed of. However, this regulation would depend on each medical school and the purpose of using clinical-log data. It is possible that students not be allowed to directly delete their clinical-log data. In case the university wants to dispose clinical-log data, this can be done by the IT unit.

Professional conduct on practicing medicine

The participants had a similar perception of professional conduct on practicing medicine is one of the other concerns regarding the HRIPA. Within this aspect, the GSM faculty members had a strongly supported that a professional conduct can be put into practice whether learning medicine with or without using IT to facilitate medical study (Table II). Having a good foundation in learning medicine would lead to a good medical practitioner. During their 4-years program, it is essential for students to demonstrate responsibility on patient information and have a good discipline in ethical principles. In professional practice and conduct, students should be able to demonstrate ongoing professional development, including history taking, physical examination, maintaining professional ethics on privacy, and confidentiality of patient information. The aspect on professional practice and conduct are embedded in clinical activities that students encounter in the clinical placements, whether online, offline, verbal, non-verbal, direct or indirect communication. Medicine cannot be practiced without having a good foundation of professional conduct. It cannot instantly be gained from the use of technology, but rather from personal development in the medical profession.

IV. Discussion

PDA accessible clinical-log can be used in any clinical placement where the network connection is available. In this way, clinical-log function can be provided in a common web browser without installing additional software application on PDA. This enables high portability and direct deployment of clinical-log function for all students only with an implementation on security (in both hardware and software mechanisms) and privacy protection for accessing this function. PDA device security has been addressed in the findings; however other security techniques can be applied which may depend on the type of PDAs. In terms of data security for PDA accessible clinical-log function, the possible and simple data security protection are having username and password protection for each user and providing access priority for different group of users. Therefore, it is possible for each user to have a unique identifier and level of data access based on the individual's authorisation in different groups, including students, the GSM faculty and educational technology specialists. Each user needs to log-on and log-off when started or terminated their session in accessing clinical-log. In order to protect clinical-log data against unauthorised access, the data security protocols with data encryption and decryption should be applied. From a technical perspective, the success of data security depends on the security technique being applied. On the other hand, the success of information privacy cannot be accomplished without applying data security techniques and professional practice.

In conclusion, the findings provide the understanding of aspects, concerns and appropriate strategy to safeguard data security and information privacy of PDA accessible clinical-log in PBL-based medical curriculum.

The recommendation for future research is in regard to information privacy of health information stored on PDA devices. There are policies to ensure information privacy of health information such as Privacy guidelines and Health Record Information Privacy Acts that is to be applied. However, mobility and connectivity of devices through Bluetooth and wireless applications will increase the risk of information security. Therefore studying how to maximise privacy and confidentiality of health information stored on PDAs would be an added value.

ACKNOWLEDGEMENT

The authors would like to acknowledge all interview participants and gratefully acknowledge all assistance of Prof. Don Iverson and Prof. Patrick Crookes, and Assumption University for scholarship support.

REFERENCES

[1] R.J. Kurth, V. Silenzio, and M.M. Irigoyen, "Use of personal digital assistants to enhance educational evaluation in a primary care clerkship," Medical Teacher, vol. 24, pp. 488-490, 2002.

[2] M. Peters, "PDAs pose WLAN concerns," Communication News, vol. 42, p. 6, 2005.

[3] S.L. Jarvenpaa and K.R. Lang, "Managing The Paradoxes of Mobile Technology," Information Systems Management, vol. 22, pp. 7-23, Fall 2005.

[4] K.T. Win, "A review of security of electronic health records," Health Information Management Journal, vol. 34, pp.13-18, 2005.

[5] A. Miller, "PDA security concerns," Network Security, vol. 2004, pp. 8-10, 2004.

[6] S. Holubar and L. Harvey-Banchik, "A Review of the Use of Handheld Computers in Medical Nutrition," Nutrition in Clinical Practice, vol. 22, pp.428-435, 2007.

[7] B. Lin and J.A. Vassar, "Mobile healthcare computing devices for enterprise-wide patient data delivery," International Journal for Mobile Communication, vol. 2, pp. 343-353, 2004.

[8] J.K. Rotich, T.J. Hannan, F.E. Smith, J. Bii, W.W. Odero, N. Vu, B.W. Mamlin, J.J. Mamlin, R.M. Einterz, and W.M. Tierney, "Installing and Implementing a Computer-based Patient Record System in Sub-Saharan Africa: The Mosoriot Medical Record System," ournal of the American Medical Informatics Association, vol. 10, pp.295-303, 2003.

[9] L.A. Hughes and G.J. DeLone, "Viruses, Worms, and Trojan Horses: Serious Crimes, Nuisance, or Both?," Social Science Computer Review, vol. 25, pp.78-98, 2007.

[10] K.T. Win and J. Fulcher, "Consent Mechanisms for Electronic Health Record Systems: A Simple Yet Unresolved Issue," Journal of Medical Systems, vol. 31, pp.91-96, 2007.

[11] B. Lopez, P.F. Kolecki, D.F. Louis, and C. Ravinowitz, "The use of a personal digital assistant Patient Encounter Log System to track procedures performed by students during a mandatory emergency medicine clerkship," Annals of Emergency Medicine, vol. 44, pp. 48-49, 2004.

[12] D.Z. Louis, S.L. Rattner, R. Cowan, M. Mei, and C. Rabinowitz, "Jefferson's Patient Encounter Log System," in *Health Policy Newsletter*, vol. 16, 2003, pp. 1-3.

[13] Wayne, "Unique Features of the Family Medicine Residency." Detroit: Detroit Medical Centre, Wayne State University, 2006.

[14] Wayne, "Wayne State University: Year II curriculum guide Wayne State University School of Medicine 2006-2007." Detroit: Wayne State University, School of Medicine, 2006.

[15] J. Mattana, M. Charitou, L. Mills, C. Baskin, H. Steinberg, C. Tu, and H. Kerpen, "Personal Digital Assistants: A Review of Their Application in Graduate Medical Education," American Journal of Medical Quality, vol. 20, pp.262-267, 2005.

[16] C.J. Bertling, D.E. Simpson, A.M. Hayes, D. Torre, D.L. Brown, and D.B. Schubot, "Personal Digital Assistants Herald New Approaches to Teaching and Evaluation in Medical Education," Wisconsin Medical Journal, vol. 102, pp.45-50, 2003.

[17] T. Grandison, S. RanjitGanta, U. Braun, and J. Kaufman, "Protecting Privacy while Sharing Medical Data Between Regional Healthcare Entities," presented at Medinfo 2007: Proceedings of the 12th World Congress on Health (Medical) Informatics; Building Sustainable Health Systems, Brisbane, Australia, 2007.

[18] A.M. Autry, D.E. Simpson, D.S.A. Bragg, L.N. Meurer, V.M. Barnabei, S.S. Green, C. Bertling, and B. Fisher, "Personal digital assistant for "real time" assessment of women's health in the clinical years," American Journal of Obstetrics and Gynecology, vol. 187, pp. 19-21, 2002.