J Med Syst (2015) 39:181
DOI 10.1007/s10916-014-0181-3

MOBILE SYSTEMS

Privacy and Security in Mobile Health Apps: A Review and Recommendations

Borja Martínez-Pérez · Isabel de la Torre-Díez · Miguel López-Coronado

Received: 20 October 2014 / Accepted: 28 November 2014 / Published online: 7 December 2014

Abstract In a world where the industry of mobile applications is continuously expanding and new health care apps and devices are created every day, it is important to take special care of the collection and treatment of users' personal health information. However, the appropriate methods to do this are not usually taken into account by apps designers and insecure applications are released. This paper presents a study of security and privacy in mHealth, focusing on three parts: a study of the existing laws regulating these aspects in the European Union and the United States, a review of the academic literature related to this topic, and a proposal of some recommendations for designers in order to create mobile health applications that satisfy the current security and privacy legislation. This paper will complement other standards and certifications about security and privacy and will suppose a quick guide for apps designers, developers and researchers.

Keywords Apps · Recommendations · Laws · Mobile health (m-health) · Privacy · Security

Abbreviations

AES	Advanced Encryption Standard
BSN	Security and privacy in Body Sensor Network
BYOD	Bring-Your-Own-Device
COPPA	Children's Online Privacy Protection Act
EHR	Electronic Health Records
EU	European Union
FTC	Federal Trade Commission
HIMMS	Healthcare Information and Management Systems Society
HIPAA	Health Insurance Portability and Accountability Act
IMEI	International Mobile Equipment Identity
IT	Information Technology
NCVHS	National Committee for Vital and Health Statistics
PHI	Personal Health Information
PKI	Public Key Infrastructure
RFID	Radio Frequency Identification
RSA	Rivest, Shamir and Adleman
SIM	Subscriber Identity Module
TLS	Transport Layer Security
USA	United States of America
VPN	Virtual Private Network

Introduction

In the last years, the significant advances in telecommunications and informatics have propitiated an incredible boost of mobile communications and wireless networks [1–8], as well as an extensive use and expansion of mobile phones, especially smartphones with new features that use these new networks such as 3G and 4G [9–11] and the combination of technologies such as transistor miniaturization, high quality graphs or compact design [12–15]. Hence, the International Telecommunication Union estimated that currently, there are a nearly 7 billion mobile subscriptions (May 2014) [16] and a

This article is part of the Topical Collection on *Mobile Systems*

B. Martínez-Pérez (✉) · I. de la Torre-Díez · M. López-Coronado
Department of Signal Theory and Communications, and Telematics Engineering, University of Valladolid, Paseo de Belén, 15.
47011 Valladolid, Spain
e-mail: borja.martinez@uva.es

I. de la Torre-Díez
e-mail: isator@tel.uva.es

M. López-Coronado
e-mail: miglop@tel.uva.es

study by Gartner said that global mobile phone reached 1.8 billion units in 2013. From those, close to 1 billion units were smartphones [17], and the numbers are increasing continuously.

The smartphones market created a new software industry: one of apps for smartphones. This industry has expanded exponentially and it is continuously in progress. In fact, there are more than 800,000 apps created only for the two most important smartphone operating systems, Apple iOS and Google Android [18, 19]. One of the different fields that have used these new devices and industry is health care. Only taking into account those mentioned operating systems, the Apple iOS' App Store [20] has more than 31,000 apps related to medicine, health and fitness whereas Android's Google play [21] has more than 16,000 medical and health care apps [22]. All these apps are included in what is known as mHealth or mobile health, defined by the World Health Organization (WHO) as "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices" [23].

However, in this run to be the first in developing and releasing a new app, some aspects have not been properly considered. Among them, privacy and security have a singular importance, especially in those apps that deal with personal and non-transferrable data, such as health applications that store patients' Electronic Health Records (EHRs) or several data regarding their health status. According to the definitions adopted by the National Committee for Vital and Health Statistics (NCVHS) of the US Department of Health and Human Services,"health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data. Confidentiality, which is closely related, refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate. Security is altogether different. It refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure" [24].

In addition, clinicians and patients are adopting mobile technologies faster than providers can protect security and privacy, which is a significant problem. According to a recent survey from Healthcare Information and Management Systems Society (HIMMS) [25], clinician use of mobile technology to collect data at the bedside rose to 45 %, up from 30 % last year, and 93 % of clinicians already use their personal smartphone to access EHR, but only 38 % did so under a formal mobile policy. The reality is that physicians and medicine students are unaware of the privacy and security aspects of the mobile applications that they use in their daily activity, as shows the study performed by Whipple et al. (2012). Such study concludes that some education in these issues is necessary because the knowledge about them is very low [26]. Not only the physicians must know about security, but also the health care organizations that have readily accepted the Bring-Your-Own-Device (BYOD) approach because of the convenience and potential cost savings associated with allowing employees to bring their own devices to work [27, 28].

Besides, in the mHealth field significant work is needed in order to overcome legal and cultural differences over privacy between nations and global regions. In this field two types of devices –medical and telecommunications– are converging, and regulators are struggling to keep up, since there are several governments and international bodies that have realized there is a problem to solve, and have moved to address the challenges of personal security and privacy in the era of smartphones and mobile applications [29].

Although there are some researches talking about privacy and security in mHealth in general [30–32], these papers do not deepen into the complexity and the global problem these aspects involve. In addition, there are few researches regarding privacy and security laws for mobile health [33, 34], but many about specific privacy or security techniques in this field [35–39]. Hence, the aim of this paper is to evaluate the current status of these features and make some guides to be followed by designers when creating an app, to satisfy the needed requisites of privacy and security. For this purpose, the authors will develop firstly a review of security and privacy laws in mHealth in developed countries, focusing on the European Union (EU) and the United States of America (USA) in order to know the main aspects to be taken into account by apps designers. Secondly, it will be developed a systematic review of the existing bibliography about the concerns and issues found over privacy and security in mobile health applications, to see the open research lines. Finally, with the knowledge obtained from the previous reviews, some recommendations regarding privacy and security aspects will be redacted, in order to satisfy the requirements stated by the considered laws.

Materials and methods

In this paper, the authors have focused only on laws of North American and European countries because of the difficulty of covering both American/European and Asian/others countries since, generally, laws from Asian countries are different from American/European (more restrictive) and it is necessary to separate them into different studies. In following works, the authors will cover security and privacy laws of Asian countries such as China or Japan, in order to assist designers to create apps for those zones. Similarly, the authors decided to focus only on the EU and USA, in order to simplify this work, selecting them for being probably the most representative zones of the occidental developed countries and two markets that are the objective of an important number of apps designers.

Another limitation is that this paper has taken into account only legal laws concerning security and privacy in mobile health, not certifications or frameworks, since there are frameworks for organizations (commercial companies, government agencies, non-profits) useful for obtaining specific certifications but written in light of the existing laws, which are the critical aspect to take into account by designers. Besides, in the industry of mobile apps, there are many apps created individually by people with no company or organization, just the person itself, so it may not be necessary getting one of those certifications. This study can also complement the existing standards in security and privacy such as ISO/IEC 27001/2013 about information security management [40], which is considered 'the foundation' by security experts worldwide. However, in this case the authors only focused on mHealth aspects.

Once exposed the limitations of this study, the methods carried out were the following: For the first part of this study, the review of security and privacy laws in mHealth in the EU and USA, the steps followed were identifying these laws and reading them carefully in order to extract the main points of each of them, trying to acknowledge common aspects and main differences. As it is mentioned before, the final objective is to summarize the laws that every apps designer should take into account when designing mHealth applications, at least for these countries. The process of identifying the laws, reading them and extracting the main points were performed by one author. The results were given to another author, who also read the laws, in order to revise the results, completing them if necessary.

The following part of this paper was the literature review of privacy and security aspects used in mobile applications in order to obey the laws. For this, the authors sought for published papers retrieved from the systems IEEE Xplore, Scopus, Web of Knowledge and PubMed, using the following search keywords: privacy AND security AND mobile AND health; privacy AND security AND health AND apps; privacy AND security AND health AND smartphones. All types of papers returned by the search were included in the study: security and privacy in apps, encryption, authentication, secure data transfer techniques, system proposals, privacy reviews, etc. Although the terms security and privacy are completely different, the authors sought for them together for two reasons: the first is that they wanted to focus on the relations between them, and the second is that, this way, the results were limited, simplifying the work. When searching for both terms separately, the results obtained were many more and, therefore, much more difficult to handle.

The only requisites needed to include a paper in the study were the following: only papers published in English were studied, the search was limited to the last 8 years, from 2007 to 2014, and the applications included must have health purposes. Figure 1 shows a flow chart of the papers selection process. Initially the systems returned a total of 570 papers, being 334 repeated. Out of the remaining papers, 67 were dismissed since they did not address the issues of this study, resulting a total of 169 relevant papers.

Since the inclusion/exclusion of papers depends on the subjective opinion of the author who performs the review, being sometimes not easy since the abstract is not clear and it can be misunderstood, we enhanced the assessment process with independent verification, as it was done in other works [41, 42]: one author developed the search of literature papers and the rest inspected the results in order to check possible errors. The authors also made a classification of the papers found following the mentioned method.

Finally, the last part of the study, the creation of privacy and security recommendations for mHealth apps designers, was performed using the results obtained in the previous parts of this research. Known the specific laws that the apps must satisfy and the techniques and technologies used for this aspects of security and privacy, the authors convened to discuss what techniques must at least be used and which of them are the most suitable in order to fulfil the laws studied.

Results

Study of the security and privacy laws in the European Union and the United States of America

The EU has one law regarding security and privacy in mHealth: the EU Data Protection Directive 95/46/EC of 1995 [43]. This is a general directive that sets the principles that the Member States should apply in their laws. Recently, at the beginning of 2012, the EU approved a draft, the General European Data Protection Regulation [44], which will substitute the previous directive in 2016 if it succeeds. There will be no need of implementing this regulation in the laws of the Member States since it will apply generally over all of them.

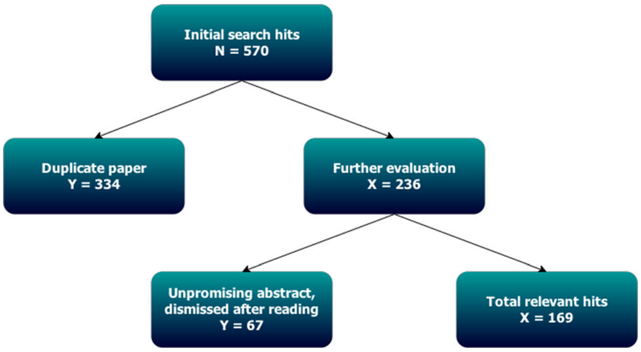

Fig. 1 Flow chart of the steps used in the literature review

With this new regulation all the Member States will be at the same stage of security and data protection.

Contrary at what happens in the EU, USA provides several laws regarding privacy and security in mHealth. The main law that applies to mHealth issues is the Health Insurance Portability and Accountability Act (HIPAA) of 1996 [45]. This law protects the privacy of the digital health information. Another important law is the Federal Trade Commission (FTC) Act [46] with its section 5. This law recently regulated aspects of mHealth privacy in the report "Mobile Privacy Disclosures: Building Trust Through Transparency" [47]. There is another significant law only applicable to children under 13, the Children's Online Privacy Protection Act (COPPA) of 1998 [48], which forbid the gathering of personal information from these children without express consent from a parent or a legal tutor. Finally, there are also State laws, but they will not be considered in this study.

Table 1 gathers a summary of the most restrictive points of the mentioned laws, sorted by the different requirements based on a study performed by Thompsons Reuters [49]. This is, when a law is more restrictive than the others with regard to a specific requirement, Table 1 shows the information of this law. If the laws are very similar regarding a requirement, then Table 1 shows the common aspects extracted from them.

Security and privacy literature review

As mentioned in the Methods section, a total of 169 relevant papers regarding privacy and security in mHealth were found. The classification of these papers by their content is shown in Table 2, which also shows the number of articles for each category in the second column.

As Table 2 shows, there are several research lines found. Below some of the most researched are enumerated, with an example of each line:

- Secure systems or solutions proposal. Sorber et al. (2012) created a wrist-worn device called Amulet that enables a trustworthy and secure path for mHealth devices to communicate with the wearer's mobile phone [50].
- Authentication techniques. Wei et al. (2012) viewed some weaknesses in two authentication methods proposed by other authors and suggested another scheme for telemedicine information systems that solves the weaknesses shown by the others [51].
- Security and privacy aspects in BSNs. In the study of Sahoo (2012), a three tier security architecture for mHealth applications is proposed, using light weight data confidentiality and authentication protocols to preserve the patients' privacy [52].
- General security or privacy aspects. Green (2013) established the necessary steps that healthcare finance leaders must satisfy to develop a good strategy to secure PHI accessed, stored, or transmitted via smartphones or tablets [32].
- Security and privacy in monitoring systems. Shin (2012) designed and evaluated a framework for securing health monitoring systems despite the security flaws of common

Table 1 Laws requisites regarding privacy and security in mHealth applications

Cover data	The data which must be covered are that information that can be used to identify a person. It includes ID numbers, physical, physiological, mental, economic, genetic, social, medical, cultural factors regarding the past, present or future of the patient.
Information requirements	Before providing their Personal Health Information (PHI), users must be informed about the identity of the person/entity that will use the PHI, the purposes of the collecting, the entity's privacy practices, whether the provision is compulsory or voluntary, the rights they have to access/modify the data and a contact method for more information or complaints. This information must be given directly to a parent or legal tutor in case of children under 13.
Consent requirements	The user/patient's consent to the data collecting must be obtained by the entity, when this collecting cannot be justified by a statutory ground. The entity is enhanced to obtain this consent written. In the case of children under 13, they cannot consent their data collection, being their parents or legal tutors the ones to do so.
Data retention	Generally, PHI should be kept only the necessary time for the purpose which was collected and must be erased once the purpose is reached. Entities must also include a clear data retention policy as part of their security procedures.
Security	The entities are required to implement and maintain appropriate technical, administrative, physical and organizational security measures to protect PHI form accidental or unlawful loss and unauthorized access or disclosure. Since health data is very sensitive, the security must be higher.
Breach notification obligations	In case of a personal data breach, the entities must notify it to the competent authority as well as the user whose data has been compromised without unreasonable delay, especially when the breach may have adversely affected to the user. In cases of massive breaches, the media should be also notified.
Data transfers	Entities need the users' consent to transfer their personal data to another entity or a third party, even when this transfer is necessary to complete one of the purposes of the data collecting, unless the transfer is allowed by law.

Table 2 Classification of the results of the literature review

Type of content	# papers
Secure system/solution proposal	23
Authentication technique/system	19
Security and privacy in Body Sensor Networks (BSNs)	11
Security and privacy in cloud computing	11
General security and/or privacy aspects	9
Security and privacy in a monitoring system	9
Security and privacy laws	9
Security in a specific place/context	7
Encryption technique	6
Security and privacy analysis of a system	6
Security and privacy in mHealth emergencies system	6
Security and privacy knowledge evaluation	6
Data transmission privacy and security	5
Security and privacy in Radio Frequency Identification (RFID) systems	5
Security and privacy evaluation of a system	5
Security and privacy in mHealth social networks	5
mHealth security guidelines	4
Security and privacy guidelines for apps	4
BSNs encryption technique	3
BSNs authentication technique	3
Health Information Technology (IT) review	3
Privacy mechanism	3
Security and privacy general aspects in apps	3
Secure data storage technique	2
Location privacy	2

personal devices, building a realistic risk model for sensor-data quality [53].

Security and privacy recommendations in mHealth applications

After reviewing the papers found, the authors were in conditions to make some recommendations to apps designers. Hence, in Table 3 there are shown the requisites that apps designers must satisfy in order to guarantee the security and privacy of the users' PHI. The table is divided into minimum requirements, those that designers must always satisfy; and recommended requirements, those which should be satisfied in order to improve security and privacy.

In addition to the requirements shown in Table 3 it is recommendable to perform periodical audits, preferably executed by external companies, of the security and privacy policy carried out by the entity (the designers). This way, designers can certify that their policies satisfy the legal requisites in privacy and security.

Discussion

Several interesting conclusions can be obtained from the analysis of the results. First of all, in light of the results of the review of the existing laws in privacy and security in mHealth it is clear that there is not a strong line and well-defined statements about this topic, at least in the EU and USA. In addition, the laws were approved long time ago (the EU Data Protection Directive in 1995 and the HIPAA in 1996), when even the term mHealth did not exist. Thus, the statements are based on the obsolete technology of these years and were applicable only in the eHealth field, but currently extended to mHealth. In practice, these laws are too open and too old, and need to be revised and reformulated taking into account the current technologies, industries and health care fields, focusing especially on mHealth and the mobile apps industry, which is continuously expanding. Although this is already happening in some cases (the General European Data Protection Regulation of the EU), the regulations are still too generalist and it seems necessary to create more specific rules mentioning possible technical mechanisms to solve security problems.

Focusing on the results of the literature review, it is easy to see that the most researched fields are those proposing secure systems (generalist or in a specific context or place), or techniques used for security and privacy such as authentication, encryption, data transmission, etc. with special mention to the aspects and techniques of BSNs, very extended lately. These new ideas are very important, but there are other very interesting fields that do not have enough research. For example, there are few security and privacy recommendations or reviews of the existing mechanisms, which is the reason of writing this paper. Location privacy also should be more researched, as the violation of this privacy is not only a violation in health care but also in every general aspect.

Papers about security and privacy in mobile apps deserve special mention, since new health apps are created every day, and they do not usually have enough security and privacy mechanisms in order to protect the users' data, such as lack of privacy policies or users' consent collection [55]. In the literature review, only seven papers focused on apps were found, four with proposed guidelines and three about security and privacy in general terms. It is really interesting the article of Albrecht et al. (2013), which proposes an app-synopsis with some guidelines for designers in order to offer transparent information about their apps, including security and privacy information [56].

Finally, with the information obtained from the literature review, it was possible to write some recommendations for apps designers about the security and privacy methods that they should follow in order to satisfy the laws of the EU and USA. Although taking into account only the minimum requisites exposed is enough for that

Table 3 Security and privacy recommendations for mHealth applications

Property	Minimum requirements	Recommended requirements
Access control	The access control to the PHI must be patient-centric. The users should be able to allow or forbid access to their information at any moment.	It is preferable to create a role-based access, giving reading possibilities to some roles and adding limitations to other ones.
Authentication	The authentication must be done with a unique ID and a password only known by the user. This ID can be linked to a Public Key Infrastructure (PKI), preferable Rivest, Shamir and Adleman (RSA) system and/or a symmetric key used for encryption.	The password used must be complex, with at least seven characters and a combination of letters and numbers, including one capitalized letter and a special character. It is better to employ multifactor authentication to complement the ID/password identification when possible: using an item the user possesses (smart key) or a physical feature such as fingerprint.
Security and confidentiality	Use Advanced Encryption Standard (AES) to encrypt PHI. The cryptographic key used must have at least 128 bits. This method offers better encryption times than other techniques [54].	It is better to improve the security using a key of 192 or 256 bits.
Integrity	At least, a symmetric key-based authentication code must be used, for example AES.	A public key-based digital signature is preferred. Under no circumstances watermarking methods must be used with medical images since they can deteriorate their quality and even provoke bad diagnoses.
Inform patients	Before the collection and use of PHI, the app should present a privacy policy informing the patients about the identity of the entity that will use the data, the purpose of the collection, the privacy methods used, the rights they have and a contact method. If the users accept this policy they give their consent to the data collection. It must include a section for minors, requiring the consent of a legal tutor.	The policy should be easy to understand, concise and clear, since users are not fond of reading large legal documents in an app. It is highly recommended to leave the policy accessible for the user at any moment in the app.
Data transfer	Use Transport Layer Security (TLS) with 128-bit encryption methods. It is also possible to use Virtual Private Networks (VPNs).	It is preferable to use TLS with 256-bit encryption methods. It is also very recommendable to show an icon in the app notifying the transfer of data.
Data retention	The retention policy should be included in the privacy policy to inform the patients. The data should be kept only the necessary time for the initial purpose.	When the purpose is achieved, the PHI must be erased and the user should be notified. The entity should provide a mechanism to let the user check that the data has been deleted.
BANs communication	At least cryptographic methods must be used in securing the BSNs for authentication and key distribution. The mobile device (smartphone) can be identified and authenticated by its International Mobile Equipment Identity (IMEI) or its Subscriber Identity Module (SIM) card number.	The user's biometric patterns user can be utilized to encrypt and decrypt the symmetric key, which can facilitate the connection of the BSNs to the mobile device.
Breach notification	In case of a PHI breach, the competent authority as well as the affected user must be notified as soon as possible (1–3 days). The entity must help the user in order to relieve the consequences the breach may have caused.	It is important to compensate the affected user in order to restore the possible damage done. In cases of breaches affecting a significant number of users, the media must be notified to inform about the problem.

purpose, we strongly recommend the use of the requisites indicated in the third column of Table 3 when possible, since PHI is very sensitive and it must be intensely protected. It is also important to mention that, although we have proposed several technical security mechanisms such as AES, RSA, VPN, etc., there are also other methods equally valid for the same goal. The authors chose those because they are well studied and commonly repeated in the papers reviewed, but the final decisions correspond to the designers.

For future work there are several research lines. It can be a good idea to extend this work by studying the laws regarding privacy and security in other zones, especially in Asian countries, in order to obtain more complete recommendations. Additionally, this work has focused on the security and privacy aspects of mobile health apps, but it does not include other important issues, such as interoperability between different systems. Hence, it can be a good idea to combine both aspects, in order to obtain a secure system but also interoperable, which implies a more complex process and study. Another future line can be the inclusion of the recommendations proposed in a real mobile app in order to evaluate the complexity and the problems that can appear in the process, trying to figure out if the disadvantages of this "extra work" (processing times, higher work load, etc.) can cause that designers opt for not integrating them in their apps, or it is simply lack of awareness of the security and privacy laws.

Acknowledgments This research has been partially supported by *Ministerio de Economía y Competitividad*, Spain.

Conflicts of interest The authors declare that they have no conflict of interest.

References

1. El Khaddar, M. A., Harroud, H., Boulmalf, M., and Elkoutbi, M., Habbani A (2012) Emerging wireless technologies in e-health Trends, challenges, and framework design issues. *International Conference on Multimedia Computing and Systems (ICMCS)* 10–12:440–445, 2012. doi:10.1109/ICMCS.2012.6320276.
2. Lin, C. F., Mobile telemedicine: a survey study. *J Med Syst* 36(2): 511–20, 2012. doi:10.1007/s10916-010-9496-x.
3. Martínez-Pérez, B., de la Torre-Díez, I., and López-Coronado, M., Mobile Health Applications for the Most Prevalent Conditions by the World Health Organization: Review and Analysis. *J Med Internet Res* 15(6):e120, 2013. doi:10.2196/jmir.2600.
4. Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., et al., A comprehensive survey of Wireless Body Area Networks. *J Med Syst* 36(3):1065–94, 2012. doi:10.1007/s10916-010-9571-3.
5. Kumar, B., Singh, S. P., and Mohan, A., Emerging mobile communication technologies for health. *International Conference on Computer and Communication Technology, ICCCT* 17–19:828–832, 2010. doi:10.1109/ICCCT.2010.5640393. Allahabad.
6. Gupta, R., and Mitra, M., Wireless electrocardiogram transmission in ISM band: an approach towards telecardiology. *J Med Syst* 38(10): 90, 2014. doi:10.1007/s10916-014-0090-5.
7. Yan, H., Huo, H., Xu, Y., and Gidlund, M., Wireless sensor network based E-health system - implementation and experimental results. *IEEE Transactions on Consumer Electronics* 56(4):2288–2295, 2010. doi:10.1109/TCE.2010.5681102.
8. Sinha, A., and Couderc, P., A framework for interacting smart objects. *Lecture Notes in Computer Science* 8121:72–83, 2013. doi:10.1007/978-3-642-40316-3_7.
9. Touati, F., and Tabish, R., u-Healthcare system: state-of-the-art review and challenges. *J Med Syst* 37(3):9949, 2013. doi:10.1007/s10916-013-9949-0.
10. Coleman, N., Mapping subscribers for better mobile networks. *GEO: connexion* 12(8):43–44, 2013.
11. Bert, F., Giacometti, M., Gualano, M. R., and Siliquini, R., Smartphones and health promotion: a review of the evidence. *J Med Syst* 38(1):9995, 2014. doi:10.1007/s10916-013-9995-7.
12. Xiao, Z., and Camino, F. E., The fabrication of carbon nanotube field-effect transistors with semiconductors as the source and drain contact materials. *Nanotechnology* 20(13):135205, 2009. doi:10.1088/0957-4484/20/13/135205.
13. Nakatani, K., New technology trends in touch panel sensing. *Proceedings of the International Display Workshops* 3:1842–1845, 2012.
14. Benfdila, A., Abbas, S., Izquierdo, R., Talmat, R., and Vaseashta, A., On the drain current saturation in carbon nanotube field effect transistors. *Nano* 5(3):161–165, 2010. doi:10.1142/S1793292010002062.
15. Bremer, M., Kirsch, P., Klasen-Memmer, M., and Tarumi, K., The TV in your pocket: Development of liquid-crystal materials for the new millennium. *Angew Chem Int Ed Engl* 52(34):8880–8896, 2013. doi:10.1002/anie.201300903.
16. ITU (2014) ICT Facts and Figures. http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf (accessed 21 September 2014).
17. Gartner (2013) Gartner Says Annual Smartphone Sales Surpassed Sales of Feature Phones for the First Time in 2013. http://www.gartner.com/newsroom/id/2665715 (accessed 21 September 2014).
18. Jones C (2013) Apple and Google Continue to Gain US Smartphone Market Share. Forbes. http://www.forbes.com/sites/chuckjones/2013/01/04/apple-and-google-continue-to-gain-us-smartphone-market-share/ (accessed 21 September 2014).
19. Canalys (2013) Top iOS and Android apps largely absent on Windows Phone and BlackBerry 10. http://www.canalys.com/newsroom/top-ios-and-android-apps-largely-absent-windows-phone-and-blackberry-10 (accessed 21 September 2014).
20. Apple (2014) iTunes. http://www.apple.com/itunes/ (accessed 21 September 2014).
21. Google (2014) Google play. https://play.google.com/store (accessed 21 September 2014).
22. Rowinski D (2013) The Data Doesn't Lie: iOS Apps Are Better Than Android. Readwrite Mobile. http://readwrite.com/2013/01/30/the-data-doesnt-lie-ios-apps-are-better-quality-than-android (accessed 21 September 2014).
23. World Health Organization (2011) mHealth: New Horizons for Health through Mobile Technologies: Based on the Findings of the Second Global Survey on eHealth (Global Observatory for eHealth Series, Volume 3). http://www.who.int/goe/publications/goe_mhealth_web.pdf (accessed 22 September 2014).
24. Cohn SP, National Committee on Vital and Health Statistics (2006) Privacy and confidentiality in the nationwide health information network. http://www.ncvhs.hhs.gov/060622lt.htm (accessed 22 September 2014).
25. HIMMS Analytics (2012) 2nd Annual HIMSS Mobile Technology Survey. http://www.himssanalytics.org/research/AssetDetail.aspx?pubid=81559&tid=131 (accessed 22 September 2014).
26. Whipple, E. C., Allgood, K. L., and Larue, E. M., Third-year medical students' knowledge of privacy and security issues concerning mobile devices. *Med Teach* 34(8):532–548, 2012. doi:10.3109/0142159X.2012.670319.
27. The Wall Street Journal – Deloitte (2013) Security and Privacy in Mobile Health. http://deloitte.wsj.com/cio/2013/08/06/security-and-privacy-in-mobile-health/ (accessed 22 September 2014).
28. Lindy Benton (2013) Marrying the BYOD phenomenon to HIPAA compliance. HIMMS. http://www.himss.org/ResourceLibrary/GenResourceDetail.aspx?ItemNumber=18909 (accessed 22 September 2014).
29. Vodafone Global Enterprise (2013) Evaluating mHealth Adoption Barriers: Privacy and Regulation – Protecting your patients privacy in a mobile world. http://mhealthregulatorycoalition.org/wp-content/uploads/2013/01/VodafoneGlobalEnterprise-mHealth-Insights-Guide-Evaluating-mHealth-Adoption-Privacy-and-Regulation.pdf (accessed 22 September 2014).
30. Hsu, C. L., Lee, M. R., and Su, C. H., The role of privacy protection in healthcare information systems adoption. *J Med Sys* 37(5):9966, 2013. doi:10.1007/s10916-013-9966-z.
31. Rosenbaum, B. P., Radio frequency identification (RFID) in health care: privacy and security concerns limiting adoption. *J Med Syst* 38(3):19, 2014. doi:10.1007/s10916-014-0019-z.
32. Green, H., Strategies for safeguarding security of mobile computing. *Healthc Financ Manage* 67(2):88–90, 2013. PMID: 23413675.

33. Gardazi SU, Shahid AA, Salimbene C (2012) HIPAA and QMS based architectural requirements to cope with the OCR audit program. Proceedings of 3rd FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (MUSIC) 2012; pp. 246–253. DOI: 10.1109/MUSIC.2012.50.
34. Luxton, D. D., Kayl, R. A., and Mishkind, M. C., mHealth data security: the need for HIPAA-compliant standardization. *Telemedicine journal and e-health: the official journal of the American Telemedicine Association* 18(4):284–288, 2012. PMID: 22400974.
35. Yeh, C. K., Chen, H. M. B., and Lo, J. W., An authentication protocol for ubiquitous health monitoring systems. *Journal of Medical and Biological Engineering* 33(4):415–419, 2013. doi:10.5405/jmbe.1478.
36. Ren, J., Wu, G., and Yao, L., A sensitive data aggregation scheme for body sensor networks based on data hiding. *Personal and Ubiquitous Computing* 17(7):1317–1329, 2013. doi:10.1007/s00779-012-0566-6.
37. Li, X., Wen, Q., Li, W., Zhang, H., and Jin, Z., Secure privacy-preserving biometric authentication scheme for telecare medicine information systems. *J Med Syst* 38(11):139, 2014. doi:10.1007/s10916-014-0139-5.
38. Chen CL, Yang TT, Chiang ML, Shih TF (2014) A privacy authentication scheme based on cloud for medical environment. J Med Syst;38(11):143. DOI: 10.1007/s10916-014-0143-9.
39. Kim, J. T., Enhanced secure authentication for mobile RFID healthcare system in wireless sensor networks. *Communications in Computer and Information Science* 352:190–197, 2012. doi:10.1007/978-3-642-35603-2_28.
40. ISO (2013) ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. http://www.iso27001security.com/html/27001.html (accessed 23 September 2014).
41. Martínez-Pérez B, de la Torre-Díez I, López-Coronado M (2014) Comparison of Mobile Apps for the Leading Causes of Death Among Different Income Zones: A Review on Literature and Apps Stores. JMIR Mhealth Uhealth;2(1):e1. DOI: 10.2196/mhealth.2779.
42. Martínez-Pérez B, de la Torre-Díez I, López-Coronado M, Sainz-de-Abajo B, Robles M, García-Gómez JM (2014) Mobile Clinical Decision Support Systems and Applications: A Literature and Commercial Review. J Med Syst;38(4). DOI: 10.1007/s10916-013-0004-y.
43. Official Journal L (1995) DIRECTIVE 95/46/EC of the European Parliament and of the Council of 24 October 1995; P. 0031 – 0050.
44. European Commission (2012) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM(2012) 11 final.
45. Pub. L (1996) Health Insurance Portability and Accountability Act of 1996. No. 104–191, 110 Stat. 1936 (1996). 42 U.S.C. § 1320d-9.
46. Federal Trade Commission Act. 15 U.S.C §45.
47. FTC Staff Report (2013) Mobile Privacy Disclosures: Building Trust Through Transparency. http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf (accessed 26 September 2014).
48. Pub.L (1998) Children's Online Privacy Protection Act of 1998 (COPPA). No. 105–277, 112 Stat. 1998. 15 U.S.C. § 6501–6506.
49. Thomson Reuters Foundation (2013) Patient Privacy in a Mobile World. A Framework to Adress Privacy Law Issues in Mobile Health. http://www.mhealthalliance.org/images/content/trustlaw_connect_report.pdf (accessed 26 September 2014).
50. Sorber J, Shin M, Peterson R, Cornelius C, Mare S, et al. (2012) An Amulet for trustworthy wearable mHealth. HotMobile - 13th Workshop on Mobile Computing Systems and Applications 2012;7. DOI: 10.1145/2162081.2162092.
51. Wei, J., Hu, X., and Liu, W., An improved authentication scheme for telecare medicine information systems. *J Med Syst* 36(6):3597–3604, 2012. doi:10.1007/s10916-012-9835-1.
52. Sahoo, P. K., Efficient security mechanisms for mHealth applications using wireless body sensor networks. *Sensors (Switzerland)* 12(9):12606–12633, 2012. doi:10.3390/s120912606.
53. Shin M (2012) Secure remote health monitoring with unreliable mobile devices. Journal of Biomedicine and Biotechnology;546021. DOI: 10.1155/2012/546021.
54. Fife, E., and Orjuela, J., The privacy calculus: Mobile apps and user perceptions of privacy and security. *International Journal of Engineering Business Management* 4(1):1–10, 2012. doi:10.5772/51645.
55. Albrecht, U. V., Von Jan, U., and Pramann, O., Standard reporting for medical apps. *Stud Health Technol Inform* 190:201–203, 2013. PMID: 23823422.
56. Silva BM, Rodrigues JJ, Canelo F, Lopes IC, Zhou L (2013) A Data Encryption Solution for Mobile Health Apps in Cooperation Environments. J Med Internet Res;15(4):e66. DOI: 10.2196/jmir.2498.