*Exploring the need for a suitable Privacy Framework for mHealth when managing Chronic Diseases**

Farad Rafique Jusob
School of Science and Technology
Middlesex University,
London UK
Email: fj105@live.mdx.ac.uk

Carlisle George
School of Science and Technology
Middlesex University
London, UK
Email: c.george@mdx.ac.uk

Glenford Mapp
School of Science and Technology
Middlesex University
London, UK
Email: g.mapp@mdx.ac.uk

Abstract. The widespread rises in chronic illnesses (e.g. diabetes, high blood pressure) have resulted in the need to find more efficient ways of managing patients with these conditions. One such way is by the use of mobile health (mHealth) technologies that can gather real time data from patients and monitor them from a distance, removing the need to be at a medical facility. These technologies can be an integral part of intelligent healthcare environments (e.g. smart homes to monitor and assist elderly patients) which are essential to reducing healthcare costs and improving efficiency. The use of mHealth, however, brings various privacy concerns and challenges. This paper reviews and examines the challenges of preserving user privacy in the context of using mHealth to manage chronic diseases. The paper first discusses mHealth, its importance in managing chronic diseases, and the associated privacy concerns. Secondly, the paper compares existing privacy frameworks applicable to mHealth. Thirdly, the key principles gathered from the frameworks are analysed in the context of their suitability for enabling adequate privacy when using mHealth for managing chronic diseases. Finally the paper argues that a new privacy framework is needed for mHealth in the context of managing chronic diseases.

Keywords: Privacy, mHealth, Self-management, Chronic Diseases, Intelligent Environments

1. INTRODUCTION

In Europe new challenges are being faced by healthcare systems, such as an increase in the elderly population (highly susceptible to chronic diseases) as well as budget cuts. The use of mobile Health (mHealth) is seen as one of the possible solutions to addressing these challenges [1]. According to the World Health Organisation [2], chronic diseases, such as diabetes and obesity, have been found to be one of the biggest challenges to worldwide healthcare systems. These diseases were responsible for over 36 million global deaths in 2008 and it was predicted that the death toll will continue to increase in the coming decade (up to 2018). mHealth services can be beneficial to managing chronic diseases by, for example, improving patient monitoring without the need to visit a health centre [3]. Mobile devices can also provide real-time data to doctors as well as suggestions to patients based on decision support systems [4]. mHealth technologies can be an important part of intelligent environments [5] that focus on providing efficient and cost-effective healthcare especially for vulnerable populations (such as the elderly). This is especially important in light of an increasing aging population, increases in chronic diseases, high cost of healthcare services and the need to use limited resources effectively. Given the sensitivity of health data, the rapid development of the mHealth sector raises concerns regarding the use of data collected from users. A report by the European Commission [1] concluded that current issues which may hinder the adoption of mHealth (based on stakeholders' views) include: data protection (including security of health data), big data, the applicability of EU legal frameworks, patient safety and transparency of information, and data privacy.

This paper will give a brief overview of mHealth and will compare various privacy frameworks, as well as privacy principles and guidelines most relevant to mHealth. The paper will then discuss the suitability of these frameworks and principles for safeguarding privacy when using mHealth to monitor chronic diseases. Finally the paper will focus on the need for a new framework for mHealth in the context of managing chronic diseases.

2. MHEALTH

Mobile Health (mHealth) is "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices"[2]. It also includes mobile applications (apps) [6,7] on smartphones that are connected to peripherals such as wearable technologies (e.g. as activity trackers or smartwatches) and medical devices [8]. Body sensors and mobile apps enable the collection of considerable medical, physiological, daily activity and lifestyle data which is used to improve personalised treatment and medication for

*Published in *Journal of Reliable Intelligent Environments, 3 (4). pp. 243-256. ISSN 2199-4668*

patients as well as enable users to manage their own health by self-assessment [1]. Mobile phones are used to improve point of service data collection, care delivery, patient communication, real time medication monitoring, and adherence support. With an estimated two thirds of the world's population (4.8 Billion) having unique mobile phone subscriptions in 2016 [9], it has been estimated that by 2020 over three quarters (75%) of the world's population (5.7 Billion) will subscribe to mobile services. The proliferation of these technologies provides the possibility to improve the safety and autonomy of patients [10].

The emergence and rapid development of mHealth has the potential to play an important role in the transformation of healthcare and increase its quality and efficiency [1,11]. mHealth solutions cover various technologies that allow for their users to measure vital signs (such as heart rate and blood pressure) and collect other medical data. The use of sensors and mobile apps to collect medical, physiological, lifestyle, daily activity and environmental data, could serve as a basis for evidence-driven care practice and research activities, while allowing patients access to their health information at any given time or place. mHealth can also support the delivery of high-quality healthcare, and enable more accurate diagnosis and treatment. It can support healthcare professionals in treating patients more efficiently as mobile apps can encourage adherence to a healthy lifestyle, resulting in more personalised medication and treatment. It can also contribute to patient empowerment as they would be able to manage their health more actively whilst still living more independent lives in their own home environment due to self-assessment or remote monitoring solutions [1, 12].

There are many different approaches and architectures to implementing mHealth (see [13, 14, 15, 16]). Differences in these architectures include types of devices, networks and communication protocols used among others. Some of these differences arguably have privacy implications. For example, in a simple mHealth architecture raw patient data can be collected from body sensors then sent to a smartphone app which constantly transmits the raw data to a care centre for analysis by health care professionals [14]. In a more sophisticated architecture the smartphone app can include intelligent patient monitoring capabilities (with decision support functionalities) that would process the raw data from sensors and only transmit relevant information to healthcare professionals, hence reducing privacy concerns by reducing the type and amount of data transmitted [14].

Figure 1 below illustrates the architecture of a simple mHealth system which arguably has the most privacy concerns (in the absence of sophisticated/intelligent patient monitoring capabilities). Data is collected from a patient using various body sensors (e.g. blood pressure monitors) or via self-readings (e.g. taking blood glucose levels). The data is then transferred to a mobile device usually to a smartphone app that has various data management functionalities. Data from the mobile device is then sent to servers or cloud storage from where it can be accessed by medical personnel and third parties (e.g. other researchers or insurance providers). In some instances data may be accessed/sent directly from the mobile app. Data can flow in more than one direction (e.g. where there is need for medical professionals/insurance providers to communicate with a patient).

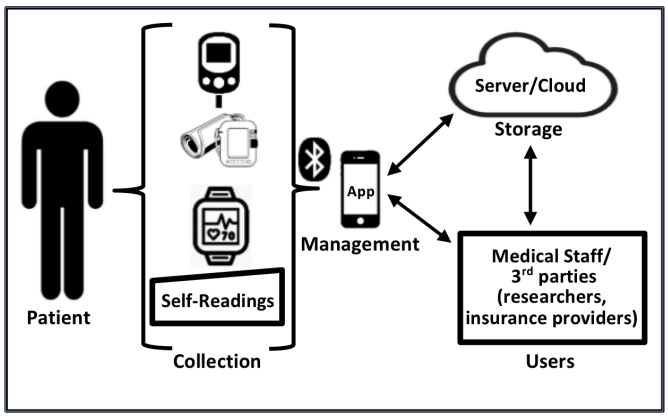

Figure 1: mHealth and its components in the context of monitoring chronic diseases

3. PRIVACY

3.1 Introduction

Privacy is a difficult concept to define, since it has been used to denote a wide number of interests including: personal information control; reproductive autonomy; access to places and bodies; secrecy; and personal development [17]. Privacy in its simplest form can be defined as a state in which one is not observed or disturbed by other people [18]. Data or information privacy from a technological standpoint is "the right of an individual to determine to what extent information is being collected about him/her as well as to what extent their information is made available to others with both personal and non-personal data" [19]. Privacy as we know it has only been around for approximately 150 years and only in recent years has information privacy become an ever growing concern.

According to Solove [18], "the need for privacy is a socially created need. Without society there would be no need for privacy." Individuals, establishments, and governments can all participate in activities that may have a negative impact on the lives of others. Privacy is the liberation of social friction and it allows for individuals to take part in activities that they would find challenging. However, privacy is not freedom from all forms of social friction, but instead, it is a safeguard. Solove [18] states that, privacy can be classified into four harmful activities: Information collection, Information processing, Information dissemination and Invasion. Firstly, information collection refers to the various entities that are able to collect information from an individual and by doing so the collection of the information can be considered a harmful action. Although not all information being collected can be harmful to the individual, certain kinds of compendium of information can be considered harmful. Secondly, information processing refers to those entities that store, combine, manipulate, search and use the collected information. Thirdly, information dissemination refers to the transferring and sharing of the individual's information which results in reduced control of the information by the individual. Lastly, invasions involve an impact directly on the individual and can result in intrusions as well as decisional interference.

The right to privacy (respect for private life) is guaranteed under Article 8 of the European Convention of Human Rights (ECHR), and in Article F(2) of the Maastricht Treaty (which established the European Union), the Union committed to respect all fundamental rights under the ECHR. The right to privacy is also guaranteed under Article 7 of the Charter of the Fundamental Rights of the European Union and

is protected as an important principle in EU Law especially Data Protection legislation (the EU Data Protection Directive 95/46/EC [20] and the new General Data Protection Regulation 2018 [21]). Privacy is especially important in the context of healthcare since under EU data protection legislation, medical data is included in a special category of data called "sensitive personal data", that is subject to stricter conditions for processing (i.e. any activity involving data).

3.2 Important Privacy Framework and principles

A privacy framework outlines core principles, best practices and solutions to protect and manage the privacy of information and people. Privacy frameworks may be used as tools to better understand and frame discussions about privacy, and their requirements [22], the latter being very important when designing and developing technological innovations such as mHealth systems. When using mHealth technologies, patients must trust that their health information is private and secure. If patients lack a sense of trust and feel that the confidentiality and accuracy of their health information is at jeopardy, they may not want to disclose their personal health information which may result in a misunderstanding of the patients' overall health status and could lead to life-threatening consequences [23]. This is one of the reasons why it is critical to ensure the privacy and security of health information. By doing so, there may be an increased sense of trust between patients and their healthcare practitioner which in turn could lead to improved diagnosis and treatment [23]. Having a suitable privacy framework for mHealth in the context of the management of chronic diseases is therefore essential to building patient trust and providing good healthcare. Research by the authors of this paper on privacy frameworks and principles concluded that several important frameworks and principles exist. Some of these frameworks are applicable in the context of healthcare and others are more general in nature. Some of the most relevant frameworks are introduced and briefly discussed below.

1) Information Systems Development Privacy Framework (2004)

According to Carew and Stapleton [24] Information and Communication Technologies (ICT) are being increasingly used in healthcare to aid the delivery, efficiency and effectiveness. This however raises a number of ethical and privacy concerns. They state that privacy is highlighted as an important and ethically charged issue, but it is frequently undervalued in literature on information systems development (ISD) and healthcare informatics. Carew and Stapleton argue that in order to provide an appropriate analysis of privacy concerns it is necessary to conduct an analysis centred on patients, the healthcare organisation as well as the technology being used. Privacy is usually seen as "a boundary control process whereby individuals control how much or little contact they have with others at a given time in a given situation and it is necessary to ensure an optimal level of privacy in order to ensure desirable behaviour"[25]. In 2004, Carew and Stapleton's Conceptual framework was developed for privacy in the context of information Systems development and takes into consideration five main categories of privacy namely: Physical, Social, Psychological, Informational and Global. Within these categories they discussed various aspects of privacy. For example under *physical,* an environmental aspect is considered, under *social,* they focus on *anonymity*, the *psychological* aspect refers to self-identity and protection, the *informational* aspect discusses use of personal information and the *global* context explains how culture affects privacy. This framework was later used in a study conducted by Carew and Stapleton [25] in a healthcare setting and they concluded that for patients, the main privacy issues are: the change of environment; the changing relationship with the clinician; and the personal information that is collected. Carew also classifies privacy in three factors, namely: *type* – Which refers to a state of desired privacy; *function* – the reasoning behind why privacy is sought after; and *contributing factor* – which refers to influence on the capability to achieve privacy.

2) HPP Best Practice Principles (2007)

The Health Privacy Project (HPP) lists ten "best practices" for employers who are developing personal health records (PHR) [26, 27, 28] as discussed below. (1) *Transparency and notice*: The entities collecting data should have explicit reasoning as to why they are providing a PHR to their patients and all policies that apply to the PHR. A policy statement or notice should be provided that clearly states how an individual's data will be processed as well as indicate how the data will be safeguarded and how individuals will be notified in the event that there is a change. (2) *Education*: Data subjects should be informed as to what are the benefits, functions, and contents of their PHR. (3) *Employees should be able to choose which content is included in the PHR*. Individuals should be allowed to define the content of their PHR, including which providers and plans contribute to it. All sources of information contained within an individual's PHR should be easily identified*; (4) Patients control access to and use of the PHR*: (a) patients should be allowed to define who can access their information. Data collection entities should not be allowed to access or use patients' individually identifiable health information from the PHR. (b) Patients should have the choice as to whether or not they wish to grant access to personal health information within their PHRs for any secondary uses. A log of who has accessed the PHR should be easily accessible to patients. (5) *Patients can assign proxies to act on their behalf*: Patients should state who should have direct access to their PHRs on their behalf as well as be allowed to grant full or partial access to their PHRs. Patients should also have the ability to reinstate and remove access rights of access. (6) *"Chain of trust": Information policies extend to business partners*: The information policies which were previously stated should comply with a series of trust agreements that third parties should adhere to. (7) *Data security*: Data processors and controllers are required to provide adequate data security in order to ensure that personal information is safeguarded. An authentication process for access to PHRs is necessary as well as a log of who has accessed the PHR. (8) *Data management*: Comprehensive data management strategies are required in order to protect the integrity of the data and the inclusions of data retention policies are necessary. (9) *Enforcement and remedies*: The data collection entities are required to ensure that all policies previously stated in the notice or policy statement are being adhered to. As well as have a system in place to notify patients of any unauthorised access to or use of their information. (10) *Portability*: PHRs should be portable to a possible extent whilst simultaneously allowing patients to update or move the data it contains.

Summary of HPP's privacy principles: HP1: Transparency and notice; HP2: Education; HP3: Patients can choose which content is included in the PHR; HP4: Patients control access to and use of the PHR; HP5: Patients can assign proxies to act on their behalf; HP6: "Chain of trust": Information policies extend to business partners; HP7: Data security; HP8: Data management; HP9: Enforcement and remedies and HP10: Portability.

3) Markle's Common Framework (2008)

The Markle Foundation initiated a project called "Connecting for Health", which congregated a vast range of stakeholders with the goal of developing a "Common Framework", a model for healthcare information exchange [29]. The Common Framework defines both policy and technical principles for healthcare information exchange in the context of managing privacy. The framework consists of the following nine principles discussed below. (1) *Openness and transparency*: Individuals have the right to know what information has been collected about them, its purpose, who can access it and where it is being stored as well as be granted access to their information should they wish to know what data has been collected in regards to them and wish to limit who can access it. (2) *Purpose specification*: The justification for which personal data will be collected should be stated beforehand, and the successive use should be limited to those purposes that were initially specified. (3) *Collection limitation and data minimisation*: Personal data should only be collected for reasons previously agreed upon and should be gathered through lawful and fair means. The collection and storage of the data should not surpass its specified purpose. Individuals should provide consent or at least understand the reasoning for collection of their personal data. (4) *Use limitation*: Personal data should not be used in any manner or form for purposes other than those initially agreed upon. (5) *Individual participation and control*: individuals should have control and access to their personal information as well as be made aware of how it is being used. (6) *Data quality and integrity*: When personal data is collected, it should be reviewed in order to ensure its relevance, accuracy, completeness and ensure it is up-to-date for the purposes for which they are to be used for. (7) *Security Safeguards and Controls*: adequate protection of personal data should be enforced through security safeguards in order to minimise and protect data from loss, unauthorised access, disclosure and modification. (8) *Accountability and Oversight:* all entities who use and control personal data should be held accountable for the implementation and enforcement of the principles. (9) *Remedies:* there should be adequate and sufficient legal and financial remedies in the event that there is a security or privacy violation.

Summary of Markle's privacy principles: MA1: Openness and transparency; MA2: Purpose specification; MA3: Collection limitation and data minimisation; MA4: Use limitation; MA5: Individual participation and control; MA6: Data quality and integrity; MA7: Security safeguards and controls; MA8: Accountability and oversight and MA9: Remedies.

4) Office of the National Coordinator for Health Information Technology (ONC) Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (2008)

In December 2008 the Office of the National Coordinator (ONC) for Health Information Technology released an important report, announcing its Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information. This ultimately led to the creation of the ONC Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information. The framework is made up of eight key principles [23]. (1) *Individual Access*: Refers to the need for Individuals to be provided with simple and appropriate access to obtain their individually identifiable health information in a readable form and format. (2) *Correction*: States that an individual should be provided with an appropriate method to dispute the accuracy or integrity of their information, and allow for the correction or to have a dispute documented if their appeals are refused. (3) *Openness and transparency*: Discusses the need for openness and transparency about policies, procedures, and technologies that may have a direct impact on individuals and their personal data. (4) *Individual choice:* Refers to how individuals should be allowed to make informed decisions about the collection, use, and disclosure of their personal data. (5) *Collection, use, and disclosure limitation:* Discusses the extent to which an individual's information should be collected, used, or disclosed only to the extent which was previously agreed upon as well as the limit of its disclosure. (6) *Data quality and integrity*: Describes how individuals should take appropriate measures to ensure that their personal data is complete, accurate, and up-to-date. (7) *Safeguards*: refer to the necessity to ensure that there is adequate protection of personal data through appropriate safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorised or inappropriate access. (8) *Accountability:* Describes how the implemented principles should be monitored in order to ensure that appropriate enforcement is taking place as well as to disclose and mitigate any nonadherence and security breaches.

Summary of the ONC's privacy principles. ON1: Individual Access; ON2: Correction; ON3: Openness and transparency; ON4: Individual choice; ON5: Collection, use, and disclosure limitation; ON6: Data quality and integrity; ON7: Safeguards; ON8: Accountability

5) Generally Accepted Privacy Principles (2008)

The Generally Accepted Privacy Principles (GAPP*)* defines privacy as "the rights and obligations of individuals and organisations with respect to the collection, use, retention, disclosure, and disposal of personal information" [30]. There are the ten generally accepted privacy principles. (1) *Management*: This principle ensures that the institution defines the documents, communications and type of accountability that is needed for their privacy policy and operation. (2) *Notice*: Ensures that notice is given to an individual (when collecting personal data) with regard to the organisation's privacy policy/procedures and the purpose for which personal data is collected and processed. (3) *Choice and consent*: This principle ensures that institutions obtain implicit or explicit consent with regard to how personal information is processed. (4) *Collection*: This refers to the collection of

personal information and the extent to which it can be used in accordance with notice given to an individual. *(5) Use, retention, and disposal*: This principle limits the use of personal information in accordance with the notice whereby an individual has provided their implicit or explicit consent. It also limits institutions from retaining an individual's information for longer than necessary and ensures adequate disposal of the information. (6) *Access*: This principle ensures that data owners have access and the ability to review and update their information when and where they deem necessary. (7) *Disclosure to third parties*: This principle limits the disclosure of an individual's information to a third party, to those mentioned in the notice and also on the basis that there is implicit or explicit consent from the individual. (8) *Security for privacy*: This principle ensures that the institution has safeguards in place to protect an individual's personal information from unauthorised access. (9) *Quality*: This principle is in place to ensure that institutions are able to store information that is accurate, complete and relevant to what was stated in the notice. (10) *Monitoring and enforcement*: This principle ensures that institutions comply with what is stated in their notice and do what is necessary to ensure that the policies and procedures are upheld.

Summary of GAPP's privacy principles. GP1: Management; GP2: Notice; GP3: Choice and consent; GP4: Collection; GP5: Use, retention, and disposal; GP6: Access; GP7: Disclosure to third parties; GP8: Security for privacy; GP9: Quality; and GP10: Monitoring and enforcement

6) A Privacy Framework for Mobile Health and Home-Care Systems (2009)

In 2009 Kotz et al [27] reviewed various privacy frameworks and principles including the ONC National framework, HPP best Principles of 1999 and HPP best practices 2007, Markle's Common Framework (2008) and CCHIT's certification criteria (2008). After the review of the frameworks they suggested that Markle's Common Framework (2008) would be the most appropriate for the research and development of mHealth systems. However, in addition to the nine principles of Markle's Common Framework they also recommended adding principles from the HPP best practices 2007 such as *Patients can choose which content is included in the PHR, Patients can assign proxies to act on their behalf* and *"Chain of trust" (i.e. Information policies extend to business partners)*. In addition, principles from the ONC National Framework such as *Individual Access, Correction, Openness and transparency* and *Individual choice* were recommended. Lastly, Kotz et al suggested that "The presence of medical sensing devices or of sensor-data collection, should not be observable by nearby parties" as they found this to be a unique privacy threat to mHealth.

Summary of Kotz et al's privacy principles. KZ1: Openness and transparency; KZ2: Purpose specification; KZ3: Collection limitation and data minimisation; KZ4: Use limitation; KZ5: Individual participation and control; KZ6: Data quality and integrity; KZ7: Security safeguards and controls; KZ8: Accountability and oversight; KZ9: Remedies; KZ10: Patients can assign proxies to act on their behalf; KZ11 "Chain of trust": Information policies extend to business partners; KZ12: Individual Access; KZ13: Correction; KZ14: Openness and transparency and Individual choice; and KZ15: The presence of medical sensing devices or of sensor-data collection, should not be observable by nearby parties.

7) Privacy by Design (2010)

Privacy by design is becoming ever more popular among regulators in the field of information and communication technologies. One example of this is its use as part of the ''General Data Protection Regulation'' (Article 25) which is set to become EU regulation in May 2018 [31]. ENISA [32] notes that "privacy by design, or its variation data protection by design, is regarded as a multifaceted concept, involving various technological and organisational components, which implement privacy and data protection principles in systems and services."

"Privacy by Design" is based on Seven Principles [33,34,35]. (1) *Proactive, not reactive; preventative, not remedial*: This principle anticipates and prevents privacy invasiveness before it occurs. This safeguards users from privacy risks and ensures that Privacy by Design comes before-the-fact, not after. (2) *Privacy as the default:* This principle seeks to ensure that privacy safeguards are in-built within the system whether or not individuals choose to use them. (3) *Privacy embedded into design:* Privacy safeguards should be implemented into the design and architecture in order to ensure that privacy is part of the system and not included as an add-on. (4) *Functionality positive-sum, not zero-sum:* This principle seeks to eliminate unnecessary trade-offs and compromises such as the reduction of privacy to accommodate enhanced security and remind system designers to consider building privacy conscious environments which can be seen as a positive sum "win-win" solution for its users rather than one that is that is zero-sum "win-lose". (5) *End-to-end lifecycle protection:* This principle is built on the basis that privacy needs to be implemented from the first moment that data is collected in order to ensure that all data is kept in a secure manner until the data is deleted. (6) *Visibility and transparency.* This principle assures all stakeholders of a system that all of its features will remain visible and transparent in order to ensure that stakeholders are aware of where the data is coming from and how it is being used. (7) *Respect for users' privacy:* This principle seeks to ensure that system developers and operators design systems where users' privacy is their main focus in order to provide systems with strong privacy defaults where data risks are reduced.

Summary of Privacy by Design principles. PD1: Proactive, not reactive; preventative, not remedial; PD2: Privacy as the default; PD3: Privacy embedded into design; PD4: Functionality—positive-sum, not zero-sum; PD5: End-to-end lifecycle protection; PD6: Visibility and transparency; and PD7: Respect for users' privacy.

8) Organisation for Economic Co-operation and Development (OECD) Principles (2013)

Internationally, the OECD Privacy Principles [22] provide the most commonly used privacy framework. They are reflected in existing and emerging privacy and data protection laws (e.g. EU data protection legislation), and serve as the basis for the creation of many privacy codes and regulations. The privacy principles defined by the OECD comprise of eight principles [22] related to personal data. (1) *Collection limitation*: Data collection should occur only with the knowledge and consent of a concerned individual (data subject); (2) *Data quality*:

Data should only collected if it is relevant and accurate for a particular purpose; (3) *Individual participation*: the individual whose data is being collected should be made aware when their information has been collected and must be able to access it if it exists; (4) *Purpose specification*: the purposes for which personal data are being collected should be specified at the time of collection. (5) *Use limitation*: Collected data must not be used for purposes other than the ones specified at the time of collection; (6) *Security safeguards*: Reasonable measures must be taken to protect data from unauthorised use, destruction, modification, or disclosure of personal information; (7) *Openness*: Individuals should be able have control over the entity who collects their data and be able to contact the entity; (8) *Accountability*: the data collector should be held accountable for failing to abide by any of the rules above.

Summary of OECD's privacy principles. OE1: Collection limitation; OE2: Data quality; OE3: Individual participation; OE4: Purpose specification; OE5: Use limitation; OE6: Security safeguards; OE7: Openness; OE8: Accountability.

9) Privacy Code of Conduct on mHealth apps (2016)

In 2016 the European Commission produced a final draft Privacy Code of Conduct on mHealth apps [36]. The aim of the code is to ensure data protection compliance and to promote good practices for app developers. At the time of writing the final draft is being reconsidered in light of review comments for amendments to the code from the Article 29 Working Party [37]. The draft code contains twelve main guidelines for app developers. (1) *User's consent*: uses must give free, specific and informed consent to the processing of their data. For health data, explicit consent must be obtained. Where consent is withdrawn, then personal data must be deleted. (2) *Purpose limitation and data minimisation*: only data needed for the functions of the app should be processed. Such processing must be for specific and legitimate purposes. (3) *Privacy by Design and Default*: During each stage of development of an app, privacy implications must be considered. The least privacy invasive choice should be the default choice (4) *Data Subjects' rights and information requirements*: Subjects must be given various rights including access to their personal data, ability to request corrections and object to further processing. (5) *Data retention*: Personal data should not be kept for longer then is necessary (6) *Security*: appropriate security measures (technical and organisational) must be adopted. (7) *Advertising in mHealth Apps*: the user must be able to authorise advertising related to personal data within the app (8) *Use of personal data for secondary purposes*: such processing must be compatible with the original purpose for which the data was collected otherwise new consent is required. Compatible purposes include further processing for scientific and historical research or statistical purposes. (9) *Disclosure of data to third parties*; There must be a legal agreement with the third party, and the user needs to be informed before disclosure. (10) *Data transfers*: rules regarding international data transfers need to be complied with. (11) *Personal data breach rules*: special rules in the code must be followed when a personal data breach occurs, including notification to the relevant data protection authority. (12) *Data gathered from children*: attention must be paid to the age limit for minors in national legislation and the most restrictive data processing approach should be taken. Further parental consent must be obtained for users under the age of 16.

Summary of Privacy Code of Conduct on mHealth principles: PC1:User's consent; PC2:Purpose limitation and data minimisation; PC3: Privacy by Design and Default; PC4: Data Subjects' rights and information requirements; PC5: Data retention; PC6: Security; PC7:Advertising in mHealth Apps; PC8: Use of personal data for secondary purposes; PC9: Disclosure of data to third parties; PC:10: Data transfers; PC11: Personal data breach; PC12: Data gathered from children.

10) General Data Protection Regulation (2018)

The General Data Protection Regulation (GDPR) is scheduled to come into force in the European Union (EU) in May 2018 updating and replacing the EU Data Protection Directive 95/46/EC (aimed at protecting the privacy of individuals and the use of personal data). While privacy (the appropriate use of information in a given context) and data protection (the management of personal information) are different concepts, in the EU the term 'data protection' also refers to privacy-related legislation/regulations [21]. The GDPR places specific obligations on data controllers and data processors in organisations (that process personal data) either within the EU or outside the EU but offering goods/services in the EU. The GDPR sets out seven principles relating to the processing of personal data. (1) *Fairness, Lawfulness and Transparency* – the processing of personal data must be done in a lawful, fair and transparent manner. Data subjects must be given information regarding the processing of their data in a transparent and intelligible manner. This should be done before any data is collected and afterwards if changes are made. The GDPR also specifies various conditions for processing personal data including (but not limited to) the consent of the data subject. (2) *Purpose Limitation*: all personal data collected by the data controller or processor must be done in a manner which is specific, explicit and legitimate for the purpose it was collected. (3) *Data Minimisation*: all personal data should be collected in an adequate and relevant manner which is limited to its purposes. (4) *Accuracy* – All personal data which is collected should be accurate and kept up to date and measures should be put in place to identify inaccurate data; (5) *Storage Limitation*: all personal data collected needs to be stored in a form which allows the identification of the data subjects for an amount of time no longer than is needed to complete the tasks which the data was collected for. However, personal data may be stored for longer so long as it will only be used for archiving purposes in accordance with Article 89(1). (6) *Integrity and Confidentiality*: All personal data collected must be processed by methods that guarantee appropriate security and privacy safeguards that will deter unauthorised and unlawful use as well as safeguard against unintentional loss or damage. (7) *Accountability*: the data controller is responsible for ensuring (and demonstrating) compliance with the principles above. This includes various data governance and accountability obligations such as: documenting the collection of consent; implementing technical and organisational measures to adequately protect personal data (e.g. pseudonymisation); taking a *data protection (privacy) by design and default approach* to data processing; conducting data protection

impact assessments; and reporting personal data protection breaches.

Summary of the GDPR principles: GD1: Fairness, lawfulness and transparency; GD2: Purpose limitation; GD3: Data Minimisation; GD4: Accuracy; GD5: Storage limitation; GD6: Integrity and confidentiality; GD7: Accountability (including Privacy by Design, ensuring Subjects' Rights).

3.3 Comparison of Relevant Frameworks and Principles

Privacy frameworks and principles can vary from one another depending on the region that they are created in as well as the context in which they are used. This has an impact on the applicability of the frameworks in different case studies since they may have been developed with the influence of different laws and ethical standards. Nonetheless, many of the frameworks and principles identified above have similarities either with identical names for principles, or similar concepts covered under different principle names.

Table 1 below gives a comparison of some of the frameworks discussed previously with the exception of Carew and Stapleton's Conceptual framework. Of all the privacy frameworks discussed earlier, Carew and Stapleton's Conceptual framework is the most unique as it was developed for privacy within information systems development and it focuses on five main categories of privacy (physical, social, and psychological, informational and global). Within these categories Carew and Stapleton focus on various aspects of privacy and this framework can be seen as an example as to how to better understand what the various elements of privacy are whereas the other frameworks all focus on specific privacy principles.

Privacy Principle	**Framework**								
	HPP (2007)	**Markle (2008)**	**ONC (2008)**	**GAPP (2008)**	**Kotz (2009)**	**PbD (2010)**	**OECD (2013)**	**PCC (2016)**	**GDPR (2018)**
Accountability		MA7		GP10	KZ7		OE8		GD7
Assignment of Proxy	HP5								
Chain of Trust	HP6				KZ10				
Choice and Consent				GP3				PC1	
Collection and Data Minimisation/ Limitation		MA3	ON5	GP4	KZ3		OE1	PC2	GD3
Correction (Accurate Data)			ON2		KZ12			PC4	GD4
Data Anonymisation and Pseudonymity									GD6
Data Management	HP8			GP1					
Data Quality and Integrity		MA6	ON6	GP9	KZ6		OE2		GD4
Education	HP2								
Enforcement and Remedies	HP9	MA9			KZ9				
Fair and Lawful Processing								PC 9 PC10 PC12	GD1
Individual Access			ON1	GP6	KZ11				GB7
Individual Choice	HP3		ON4		KZ13				
Individual Participation and Control	HP4	MA5			KZ5		OE3	PC4 PC7	GD1
Medical sensing devices not made observable by other parties					KZ14				
Notice				GP2					GD1
Openness and Transparency	HP1	MA1	ON3		KZ1	PD6	OE7	PC9 PC11	GD1
Portability	HP10								
Privacy by design and default						PD1─7		PC3	GD7
Purpose Specification of data collection		MA2		GP5	KZ2		OE4	PC2	GD1
Security Safeguards and encryption	HP7	MA8	ON7	GP8	KZ8		OE6	PC6	GD6
Storage Limitation	HP8			GP5				PC5	GD5
Use Limitation		MA4	ON5	GP7	KZ4		OE5	PC8	GD2

Table 1 - Comparison of Privacy Frameworks and Principles

4. Privacy and mHealth

4.1 Introduction

Safeguarding personal data and addressing privacy concerns is an important aspect of mHealth. According to the European Commission [1], various studies have found that individuals are mainly concerned with the way personal data is collected and processed (e.g. in one study 82% of the respondents expressed concerns that wearable technology will invade their privacy). Kemp and Moore [17] state that when dealing with health data, privacy should be mandatory. Health and wellness apps which are currently available for most smartphones are usually developed for consumers who want to personally track and evaluate their health. According to a study conducted in 2013 by a privacy advocacy group, an evaluation of over forty-three health and wellness apps found that approximately one third of them send user data to entities not covered by their privacy policies and nearly fifty percent of the freely available apps share personally identifiable information with advertisers, with the vast majority not using any form of encryption on their users' data [38]. Another study found that all free apps and only a few paid apps surveyed used encryption to protect data stored on smartphones [39].

The phenomenon of mHealth raises particular concerns regarding the privacy of health/medical data due to various reasons. Firstly, the use of mHealth involves the *collection of a huge volume of medical data* about the patient as many mHealth devices collect data continuously over extended periods of time. Secondly, mHealth allows a broad range of health-related information to be collected, including physiological data and data on patients' lifestyles and activities. Lastly, mHealth enables a broad range of health-related apps to share data with health providers (as in a traditional doctor-patient relationship) and with insurance companies [40]. In the context of mHealth, managing privacy is a complex issue: *patients need control* over the collection, recording, dissemination, and access to their mHealth data [28]. Generally, patients can regulate who has access to their personal health information through the giving of informed consent. Informed consent gives patients appropriate knowledge of what data are being collected, how they are stored and used, what rights they have to the data, and what the potential risks of disclosure could be. However, technological literacy limits user's understanding of the true threats and advantages of technology. Because of the limitation of some users regarding technological literacy, it is necessary to develop mHealth systems that allow patients added *control* over their data such as, what data is collected and who has permission to *access* it [41].

4.2 Privacy concerns/challenges for mHealth and managing chronic diseases

As discussed above, mHealth used in any context raises many privacy concerns such as: *the high volume of data collection*; *lack of data control*; *accessibility of data*; and *anonymity*. In the context of the self-management of chronic diseases there are additional privacy concerns that also need to be addressed. A case study done by Avancha et al [28] outlined the various processes a patient with a chronic illness is expected to undergo during a typical day. From this case study it was possible to identify the following privacy concerns: *Continuous Monitoring* – from a wearable device that tracks activity level; *Lack of Encryption for data transmission* – e.g. the communication between a wearable device and mobile phone; *Data Quality* – the need for adequate checks to ensure manual data input is complete and has no missing fields; *Profiling* – e.g. use of location data to identify user habits; *Data Use and Sharing* – the system sharing data with the patients' health care practitioner as well as with an insurance company.

Further, *Confidentiality* is essential in the healthcare context to ensure that medical data (transmitted/stored) or other health-related communications are not accessed by or disclosed to unauthorised entities [42]. *Invisibility* arises due to the fact that as the user becomes accustomed to body sensors and monitoring technology his/her perception of the invasiveness of the technology is diminished rendering it almost invisible to him/her [43]. Mobile phones allow for a variety of data to be collected through the use of cameras, microphones and their in-built GPS. The data collected from these devices can also disclose various habit and routines and can allow for data to be collected without their users even being aware of it, giving mobile devices the possibility to become one of the most widespread *Surveillance* tools [44].

mHealth data falls under the category of "sensitive data" as it can reveal an individual's health conditions. Due to the sensitivity of the data generated by the use of mHealth, the *misuse or abuse of personal information* raises serious concerns as it may affect an individual's fundamental rights such as the right to privacy and non-discrimination as well as having an impact on their social environment. It is therefore necessary for additional safeguards to ensure that risks of misuse or abuse are minimised [45]

A study by Krent [46] argues that, there may be discrimination against diabetics because fainting caused by a sudden drop in blood sugar may cause a safety risk to others. As a result, diabetics often face discrimination at work, in school, and even in prison. Krent [46] adds that people with diabetes feel that their health records and information should have adequate privacy due to fears of: the possibility of it being used in legal proceedings; its disclosure to public health researchers; the possibility of it being accidentally disclosed; the impact it may have on their insurance coverage and eligibility as well as health insurance; and employment discrimination (which could result in *unauthorised or unanticipated data use*).

Table 2 below lists various events using mHealth to monitor chronic diseases and the associated privacy concerns.

Process	Privacy Threat/Concern
Data collection and activity monitoring using wearables or sensors.	- Continuous Monitoring [28] - Volume of Data Collection [40] - Invisibility [43]
Transmission of data (e.g. between wearable device and mobile phone, or phone and server)	- Data Security [40] - Encryption [28, 40] - Confidentiality [32]
Location tracking using mobile phones	- Profiling [28] - Surveillance [44]
Sharing of data with healthcare practitioners and third parties (including researchers, insurance providers)	- Data Use (Unauthorised or Unanticipated) [45] - Sharing of data [28] - Information misuse/abuse [45]
Manual data Input	- Data Quality [28]
Use of Mobile Apps	- Encryption [39] - Anonymity [24] - Data Control [41] - Accessibility [41] - Disclosure risks[40]
Doctor to Patient Communication	- Confidentiality [42]

Table 2: Privacy Threats/Concerns –mHealth and Chronic Diseases

Privacy Concerns for mHealth and Chronic Diseases	Framework								
	HPP (2007)	Markle (2008)	ONC (2008)	GAPP (2008)	Kotz et al (2009)	PbD (2010)	OECD (2013)	PCC (2016)	GDPR (2018)
Accessibility of Data	HP4	MA5	ON1	GP6	KZ11	PD1-7	OE5	PC6	
Anonymity								PC3	GD6
Confidentiality			ON5		KZ3	PD1-7		PC3	
Continuous Monitoring									
Data Control	HP3	MA5	ON4		KZ13	PD1-7	OE7	PC4	
Data Quality		MA6	ON6	GP9	KZ6		OE2	PC4	GD4
Data Security	HP7	MA7	ON7	GP10	KZ7	PD1-7	OE6	PC6	GD6
Data Use		MA4	ON5	GP7	KZ4		OE5	PC8	GD2
Disclosure risks	HP4	MA2	ON5	GP5	KZ2		OE6	PC9, PC10	GD6
Encryption						PD1-7		PC3	GD6
Information misuse/abuse	HP6	MA2	ON5	GP5	KZ2	PD1-7	OE4	PC6	GD7
Invisibility									
Profiling						PD1-7			
Sharing of Data	HP4	MA5	ON5		KZ5	PD1-7	OE5	PC1, PC10	GD2
Surveillance									
Volume of data collection		MA3	ON5	GP4	KZ3		OE1	PC2	GD3

Table 3: Privacy Frameworks and how they address privacy concerns for mHealth and Chronic Diseases

5. THE NEED FOR A PRIVACY FRAMEWORK FOR MHEALTH AND CHRONIC DISEASES

5.1. Current privacy frameworks, mHealth and chronic diseases

Table 3 (above) lists privacy threats and concerns when using mHealth to monitor chronic diseases (which were identified in Table 2) and demonstrates how current privacy frameworks address these threats/concerns.

From Table 3 above, arguably, current privacy frameworks do not adequately address the privacy concerns regarding the self-management of chronic diseases when using mHealth solutions.

Figure 2 (below) illustrates various events in an mHealth scenario where data is processed (i.e. inputted, collected, transmitted, used etc.). It also highlights the key areas that give raise to privacy threats and concerns (indicated by letters in circles).

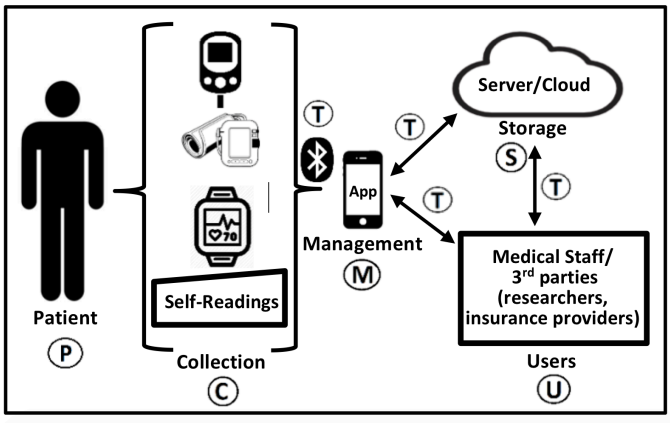

Figure 2 – Events in processing mHealth Data

The events as shown in Figure 2 include: Manual input of data from a patient (P); the collection of data from body ensors (C); the transmission of data between different stages (T), the management of data on a smartphone app (M); the storage of data in the cloud (S); and the use of data by various different types of users (U). The privacy concerns associated with each of these events are further discussed below.

Manual input of data from a patient (P): One main privacy threat/concern is raised here namely, data quality. The issue of data quality arises from the patient (data source) due to the fact that the patient may sometimes have to manually input data (e.g. from blood glucose readings) and by doing so there is always a possibility of making errors and collecting incorrect data.

The collection of data from body sensors (C): Five main privacy threats/concerns are raised here namely: data quality; continuous monitoring; volume of data collected; surveillance; invisibility. Data quality concerns arise since body sensors used in a home environment sensors may not provide the same accuracy compared to sensors used in a medical facility. Due to the fact that wearable devices and sensors are used throughout the day the concern of continuous monitoring arises as well as the issue of the volume of data collected as these devices monitor their users 24/7 and are able to collect various types of data. This brings the additional concern of surveillance as these devices allow for close observation of their data subject. As noted previously, invisibility will arise where a patient becomes accustomed to the presence of monitoring technologies (e.g. body sensors) due to constant use, hence diminishing his/her perception of their invasiveness and making them almost invisible.

The transmission of data between different stages (T): The privacy threats/concerns that arise are: the lack of adequate data security measures such as data encryption and data anonymity, leading to unauthorised access/disclosure of information in transit.

The management of medical data on a smartphone app (M): Here there are seven main privacy threats/concerns namely: lack of data security; lack of data encryption; profiling; lack of anonymity; accessibility of data; potential risk of disclosure; and surveillance. The issues raised all relate to the use of mobile apps where data from the sensors is processed (e.g. stored, used and transmitted). Studies [28, 38, 39] have shown that most mobile apps relating to mHealth have inadequate or a lack of data encryption and security. In addition to security and encryption issues, these apps have been found to share individuals' data without their consent and

with parties not mentioned in their privacy policy which results in issues such as unauthorised disclosure. Other issues such as profiling arise from the ability of these apps to collect a large volume of data from their users over long timeframes (e.g. location data which could allow for user profiling based on frequently visited locations). The issue of accessibility of data can occur when users are unable to have full access to the data collected from them as well as the inability for them to modify or delete personal data.

The storage of data in the server/cloud (S): Here five main privacy threats/concerns that are raised namely: data security; data encryption; lack of data anonymity; lack of data control; and accessibility of data. When data is stored in the cloud the accessibility and control of this data may be determined by the cloud storage provider which could limit users from being able to access their information as well as not being able to control what is done with their data once it is stored there. The issue of lack of data security, data encryption and data anonymity may be raised since this heavily relies on service providers, their agreements with application developers and their privacy/security policies.

The use of data by various different types of users (U): There are six main privacy threats/concerns that are raised here namely: limitation of data use; sharing of data; confidentiality; lack of control; accessibility of data; and information misuse and abuse. These issues arise due to the fact that data users may process information beyond what was initially specified and agreed upon during data collection. Data may be accessed by a variety of users (e.g. different kinds of health professionals, organisations/bodies authorised by law, researchers etc), hence threating the traditional one–to-one doctor-to-patient confidential relationship.

Table 4 below summarises the privacy concerns/threats at different events in an mHealth scenario.

Privacy Threat/ Concern	**Data processing events in mHealth**				
	(P)	(C)	(M)	(S)	(U)
Accessibility of Data			x	x	x
Anonymity			x	x	
Confidentiality					x
Continuous Monitoring		x			
Data Control				x	x
Data Quality	x	x			
Data Security			x	x	
Data Use (Limitation)					x
Disclosure risks			x		
Encryption			x	x	
Information misuse/abuse					x
Invisibility		x			
Profiling			x		
Sharing of Data					x
Surveillance		x	x		
Volume of Data Collection		x			

Table 4: Privacy Threats/ Concerns at data processing events in mHealth

6. Conclusions

The need for intelligent environments aimed at the provision of healthcare will continue to rise, especially in view of many factors such as: increases in aging populations and chronic diseases, costly healthcare, the need to use scarce resources efficiently, and the availability of new technologies. mHealth solutions can play an integral part of intelligent environments aimed at healthcare. The foregoing discussions in this paper have arguably demonstrated that existing privacy frameworks do not adequately address the privacy concerns of patients when using mHealth in the context of managing chronic diseases. The paper has also identified specific events in an mHealth scenario where users have privacy concerns and how each of these concerns are addressed by existing privacy frameworks. This paper asserts that there is a need to design a suitable privacy framework for the use of mHealth to manage chronic diseases. The design of any new privacy framework for mHealth in that context must address the privacy threats at each of the mHealth events identified in the discussions above. A new privacy framework would also consider other issues aimed at supporting privacy such as: patient education; patient feedback; use of privacy enhancing technologies; use of privacy by design principles; and the continuous evaluation of processes and procedures. The work completed in this paper sets the stage for the development for a new privacy framework, as the next phase in an ongoing research project undertaken by the authors.

References

1. European Commission (2014) Green Paper on mobile Health ("mHealth"). Brussels, 10 April 2014, COM(2014) 219 final.

2. WHO (2011) "mHealth – New horizons for health through mobile technologies, Global Observatory for eHealth series – Volume 3" (**online**) www.who.int/goe/publications/goe_**mhealth**_web.pdf. Accessed 15 Nov 2016

3. Estrin D and Sim I (2010) Open mHealth Architecture: An Engine for Health Care Innovation, Science 330:759-760.

4. Klonoff DC (2013) The current status of mHealth for diabetes: will it be the next big thing?, Journal of diabetes science and technology, 7:749-758.

5. Augusto J, CallaghanV, Kameas A, Cook D and Satoh I (2013) Intelligent Environments: a manifesto. Human-Centric Computing and Information Sciences, 3(12), doi: 10.1186/2192-1962-3-12.

6. Martinez-Perez, B., de la Torre-Diez, I., Lopez-Coronado, M., Sainz-de-Abajo, B., Robles, M., and Garcia-Gomez, J. (2014). Mobile clinical decision support systems and applications: A literature and commercial review. *Journal of Medical Systems, 38*(1) doi:10.1007/s10916-013-0004-y

7. Grindrod, K., Boersema, J., Waked, K., Smith, V., Yang, J., and Gebotys, C. (2017). Locking it down: The privacy and security of mobile medication apps. *Canadian Pharmacists Journal / Revue Des Pharmaciens Du Canada, 150*(1), 60-66. doi:10.1177/1715163516680226

8. Karim (2014) ICT: Wearable Technology – KARIM Foresight Report. INTERREG IV B – 207G, France. (**online**) http://www.karimnetwork.com/wp-content/uploads/2014/11/Wearable-Technology-Final_November2014.pdf Accessed 03 Jul 2017

9. GSMA (2017) The Mobile Economy 2017. (**online**) https://www.gsma.com/mobileeconomy/ Accessed 03 Jul 2017

10. Becker S, Miron-Shatz T, Schumacher N, Krocza J, Diamantidis C and Albrecht U (2014), mHealth 2.0: Experiences, Possibilities, and Perspectives, JMIR mHealth and uHealth, 2:24.

11. Malvey, D. M., and Slovensky, D. J. (2014) mHealth: Transforming Healthcare, Springer.

12. Conroy MK (2015) Connecting Patients to mHealth Apps to Enhance Self-care Management, Home healthcare now, 33: 437.

13. Saleem, S., Ullah, S., and Kwak, K. (2011). A study of IEEE 802.15.4 security framework for wireless body area networks. *Sensors, 11*(2), 1383-1395. doi:10.3390/s110201383

14. Varshney, U. (2014). A model for improving quality of decisions in mobile health. *Decision Support Systems, 62*, 66-77. doi:10.1016/j.dss.2014.03.005

15. Tmar-Ben Hamida, S., Ben Hamida, E., and Ahmed, B. (2015). A new mHealth communication framework for use in wearable WBANs and mobile technologies. *Sensors, 15*(2), 3379-3408. doi:10.3390/s150203379

16. Albuquerque, S. L., and Gondim, P. R. L. (2016). Security in cloud-computing-based mobile health. *IT Professional, 18*(3), 37-44. doi:10.1109/MITP.2016.51

17. Kemp R and Moore AD (2007) Privacy, Library Hi Tech, 25:58-78

18. Solove DJ (2006) A Taxonomy of Privacy. University of Pennsylvania Law Review. 154:477-560.

19. Araujo I (2005) Privacy mechanisms supporting the building of trust in e-commerce, DOI: 10.1109/ICDE.2005.263.

20. European Union (1995) Directive 95/46/EC 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 (**online**) http://www.refworld.org/docid/3ddcc1c74.html Accessed 17 October 2017

21. IAPP Information Privacy Centre (2011) Glossary of Common Privacy Terminology. (**online**) https://iapp.org/media/pdf/certification/CIPP_Glossary_0211updated.pdf. Accessed 07 Jul 2017.

22. Organization for Economic Cooperation and Development. (2013), OECD Privacy Principles. (**online**) https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Accessed 03 Apr 2017.

23. Office of the National Coordinator for Health Information Technology. (2008), Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information. (**online**) https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf. Accessed 07 Apr 2017.

24. Carew PJ and Stapleton L (2005) Towards a Privacy Framework for Information Systems Development in Springer US, DOI: 10.1007/0-387-28809-0_8

25. Carew PJ and Stapleton L (2005) Privacy, patients and healthcare workers: a critical analysis of large scale, integrated manufacturing information systems reapplied in health,16th IFAC World Congress, 38:1–6

26. Health Privacy Project (2007) Summary of HPP Best Principles. (**online**) https://www.slhd.nsw.gov.au/pdfs/Summary_of_HPPs.pdf. Accessed 05 Jul 2017

27. Kotz D, Avancha S and Baxi A (2009) A privacy framework for mobile health and home-care systems, ACM.

28. Avancha S, Baxi A and Kotz D (2012) Privacy in mobile technology for personal healthcare, ACM Computing Surveys (CSUR), 45:1-54.

29. Markle (2010) Connecting for Health Common Framework for Health Information Exchange, (**online**) https://www.markle.org/publications/274-connecting-health-common-framework-health-information-exchange Accessed 15 Nov 2016

30. Prosch M (2008) "Protecting personal information using Generally Accepted Privacy Principles (GAPP) and Continuous Control Monitoring to enhance corporate governance, International Journal of Disclosure and Governance, 5:153-166.

31. Nordgren A, Institutionen för kultur och kommunikation, Linköpings universitet, Filosofiska fakulteten and Centrum för tillämpad etik (2015) Privacy by Design in Personal Health Monitoring, Health Care Analysis, vol. 23, no. 2, pp. 148-164.

32. ENISA (2017) Privacy by Design. (**online**) https://www.enisa.europa.eu/topics/data-protection/privacy-by-design.Accessed 09 Jul 2017

33. ENISA (2014) Privacy and Data Protection by Design – from policy to engineering. (**online**) https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport Accessed 10 Jul 2017

34. Everson E (2016) Privacy by design: taking ctrl of big data, Cleveland State Law Review, 65:27.

35. Cavoukian A (2010) Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D. Springer. DOI 10.1007/s12394-010-0062-y.

36. European Commission (2016), Privacy Code of Conduct on mobile health apps (**online**) https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps accessed 17 October 2017

37. Clemence, B., Walkinshaw, Z.V., Mulryne, J. and Dickinson, R. (2017). WP29 Reviews the European Draft Code of Conduct on Privacy for Mobile Health Apps (**online**) http://www.digitalhealthdownload.com/2017/05/wp29-reviews-european-draft-code-conduct-privacy-mobile-health-apps/ accessed 17 October 2017

38. Ackerman L (2013) Mobile Health and Fitness Apps and Information Privacy. Privacy Rights Clearing House

39. McCarthy, M. (2013). Experts warn on data security in health and fitness apps. *BMJ : British Medical Journal, 347*(sep13 1), f5600-f5600. doi:10.1136/bmj.f5600

40. Steinhubl SR, Muse ED and Topol EJ (2015) The emerging field of mobile health, Science translational medicine,Vol 7.

41. Arora, S., Yttri, J. and Nilse, W.(2014) Privacy and Security in Mobile Health (mHealth) Research, Alcohol research: current reviews, 36:143-151.

42. Harvey MJ and Harvey MG (2014) Privacy and security issues for mobile health platforms, Journal of the Association for Information Science and Technology, 65:1305-1318.

43. Brey P (2005) Freedom and privacy in Ambient Intelligence. Ethics and Information Technology, 7:157-166.

44. Shilton K (2009) Four billion little brothers?: privacy, mobile phones, and ubiquitous data collection, ACM, New York

45. European Commission (2011) Advice paper on special categorie s of data ("sensitive data"). (**online**) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf. Accessed 15 Jul 2017.

46. Krent H (2008) Whose Business Is Your Pancreas? Potential Privacy Problems In New York City's Mandatory Diabetes Registry.