Risk Analysis of Residual Protected Health Information of Android Telehealth Apps

Completed Research Full Paper

Stacy Miller
University of South Alabama
sam1522@jagmail.southalabama.edu

William Bradley Glisson
Sam Houston State University
glisson@shsu.edu

Matt Campbell
University of South Alabama
mattcampbell@southalabama.edu

Scott Sittig
University of South Alabama
sittig@southalabama.edu

Abstract

Telehealth apps are growing at a rate faster than regulatory legislation and guidelines can keep pace. As a result, app developers, healthcare providers, and individual app users are left without a clear understanding of the rights and responsibilities of each party involved. Use of Telehealth apps may leave the end users' personal health information vulnerable. Improper security within the app may leave the app provider and healthcare providers at risk legally. The goal of this paper is to examine the regulatory framework and regulatory guidance which applies to telehealth apps. In addition, a series of three case studies were conducted to examine the prevalence and nature of residual personal health data from these telehealth apps. In two of the three case studies patient health data was recovered through the app in the form of various artifacts.

Keywords (Required)

Risk analysis, mHealth, residual data, PHI, Android

Introduction

The increasing reliance on technology is influencing almost every aspect of modern society, and healthcare is no exception. According to recent studies, 85% of healthcare providers use smart phones during work or training, and the majority of this time is spent using apps (Ozdalga et al. 2012). Almost half of adults in America own smart phones, and half of those adults report having used their phone for retrieving health information (Carroll et al. 2017). There are over 20,000 healthcare related apps across the various mainstream app markets, the majority of which are currently unregulated (Colorafi and Bailey 2016; Lewis and Wyatt 2014). While governing rules and regulations regarding technology currently exist, they are being outpaced by the capabilities of the technologies themselves. In a similar fashion, the healthcare industry has been slow to change and adapt to the robust technology capabilities. Fines for failure to follow HIPAA guidelines can range from $100 to $50,000 per violation and a mistake as simple as disabling a network firewall can cost $400,000 (Goldstein and Pewen 2013). While there are many risks inherent with technology use in healthcare, adoption is becoming more widespread (Washington et al. 2017), even as responsibilities become more diffuse and less clear (Larson 2018).

The definition of telemedicine is evolving, however, at its core it is classified as the delivery of remote healthcare and clinical services leveraging telecommunications technology (Sood et al. 2007). However, protected health information (PHI) is protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Goldstein and Pewen 2013)and the Health Information Technology for Economic and Clinical Health (HITECH) Act (Washington et al. 2017), both of which govern the

healthcare providers. The HITECH Act does include regulations for those providing information technologies for healthcare but are designed for electronic health records and governance of information contained therein, and not the personal electronic devices of individuals.

Telehealth and Telemedicine apps can potentially pose a significant risk to consumers. This risk is connected to the electronic PHI (ePHI) contained in and transmitted by these apps. Research into the new and growing field of telemedicine predominantly focuses on the risks from the healthcare provider perspective (i.e. not being able to verify patient conditions, doctors giving advice on matters outside their area of expertise, admissibility of telemedicine in court, etc.) or the forensic aspect of the apps, and not on the HIPAA side of risk (Azfar et al. 2015; Lateef 2011; Ozdalga et al. 2012; Plachkinova et al. 2015; Saleem et al. 2008).

Literature Review

Many related governmental agencies use conflicting or inexact definitions regarding mobile devices. With contradictions in the terminology, it can be difficult to assess which rules or guidelines, if any, apply to which apps. With regulatory overlap, it may be difficult to ascertain which sets of guidelines or procedures are relevant. This situation leads to problems such as where similar apps are governed very differently, or common apps are suddenly inappropriate to use. For example, a patient calling their provider on the patient's personal cell phone does not generally require any additional effort or infrastructure, but a patient video chatting with their provider does (Larson 2018; Lee et al. 2016).

One of the problems with conducting research within this field is the combination of vague regulatory guidance and overlapping agencies. According to HIPAA, for instance, it is both reasonable and appropriate for app developers to encrypt or otherwise protect patient data, but many still fail to do so (Thilakanathan et al. 2016). While development that is not security focused is not a central issue to healthcare and related areas, it is particularly salient due to PHI.

Recent research in the field telemedicine/telehealth has focused on development of and integration mHealth apps (Azfar et al. 2015; Grispos et al. 2013, 2014; Plachkinova et al. 2015). This term applies to a wide variety of health related apps including those used solely for reference purposes or casual health tracking, such as fitness and calorie counting apps (Azfar et al. 2015; Plachkinova et al. 2015). Neither one of these types of apps appear to fall under regulatory guidance (Larson 2018; Washington et al. 2017). This section defines the terms telemedicine, telehealth, and mHealth (mobile health) and explores what laws, rules, and regulations apply to this type of technology.

In our research, we draw a distinction between mHealth apps, telehealth apps, and telemedicine apps. The broadest category of the three is mHealth. It is a type of healthcare app involving the use of cell phones (mainly smartphones) for reference or personal care, and can include non-clinical care such as fitness tracking, period tracking, calorie counting, or hospital location (Ali et al. 2016). Most of the healthcare related apps available on the major cell phone markets, such as Google Play or the Apple app store, fall into the very broad mHealth category (Ozdalga et al. 2012). Broadly speaking, these apps carry a level of risk for the consumer similar to non-health specific apps, such as social networking and cloud storage apps (Plachkinova et al. 2015). These apps can be divided into four categories: patient care and monitoring; health apps for general reference; communication, education, and research; and physician or student reference apps (Ozdalga et al. 2012).

The second category of healthcare apps is Telehealth. Telehealth apps are apps which support the communication between individuals and healthcare providers (Dinesen et al. 2016). Telehealth is the technological equivalent to having an appointment with a health care provider and may involve the transmission of ePHI via the app. This information may include demographic data, medication lists, health history, insurance policy information, and other personally identifying data.

The final category of healthcare apps is telemedicine which are apps to assist with the remote delivery of healthcare and clinical services (Dorsey and Topol 2016). As technology grows telehealth and telemedicine apps are becoming very similar and may become one category in the near future (increasing the need to conduct proper forensic analysis of protected health information).

To add to the regulatory confusion, some telehealth apps fall under a variety of legal regulations or guidelines like traditional medical devices, while others do not (Goldstein and Pewen 2013; Lee et al. 2016; Lewis and Wyatt 2014; Washington et al. 2017). Telehealth regulation falls under the guidance of several government agencies, including FDA, Federal Trade Commission (FTC), and Federal Communications Commission (FCC) (Marcoux and Vogenberg 2016). The FDA has released nonbinding recommendations which cover mobile apps. These guidelines have been updated as of 2015 to inform developers of the FDA's guidance concerning the function of an app over the platform. As such, the regulations will apply to "only those mobile apps that are medical devices and whose functionality could pose a risk to a patient's safety if the mobile app were to not function as intended" (Larson 2018; Marcoux and Vogenberg 2016).

These guidelines indicate that it is the software and not the hardware that determines the classification. Furthermore, the FDA specifies that mobile apps may be classified as medical devices if they are "specifically marketed to help patients document, show, or communicate to providers potential medical conditions" regardless of whether the app is labeled as being specifically for medical use or not (Larson 2018; Marcoux and Vogenberg 2016). This guidance includes apps with a primary purpose of communicating with a healthcare provider over video or by sending messages and pictures. Educational and informational apps are *not* considered medical devices, including those for both general reference and patient education, and will not be governed by the FDA (Larson 2018; Marcoux and Vogenberg 2016).

HIPAA rules cover healthcare providers and incorporate requirements for confidentiality, privacy, and security regarding PHI. HIPAA also covers rules for business associates (Goldstein and Pewen 2013). The HITECH act guidelines expand HIPAA and cover the use of electronic data in healthcare. These guidelines specify that while healthcare providers are considered covered entities who must abide by these regulations, business associates who work with providers and handle ePHI are also subject to regulations. Business associates can face the same civil or criminal penalties as healthcare providers (Washington et al. 2017).

The business associates rule expands the explanation of business associates, contracts, definitions, and responsibilities. These guidelines require that while it is the obligation of the healthcare provider to abide by the HIPAA privacy rule, any other business associations must meet the same security and encryption standards. These protections include providing security and training to guarantee the privacy, accuracy, and availability of ePHI (Goldstein and Pewen 2013). The regulation requires business associates and providers to form a Business Associate Agreement (BAA) that specifies how the data will be handled and protected (Allen et al. 2014).

A legal example shows that not all technologies are permitted for use as telehealth. According to a news report (Lee et al. 2016), the Oklahoma medical board ruled in January 2014 that Skype could not be used by medical professionals for the purposes of treatment or diagnosis. This article explains that while Microsoft has some form of BAA, Skype is not included in the agreement. In this case, the provider faced reprimand for failing to obtain a BAA prior to using the service to provide care. This ruling reiterates the importance of having a BAA between the healthcare provider and the company providing the software, and that not all technology may be used in the course of providing healthcare. Researchers have published (Barmpatsalou et al. 2013) a review of mobile forensic practices and methods which showcased how data was acquired. These methods include manual, logical, and physical extractions. The authors also discuss differences in operating systems and types of data acquired from an analysis.

Several authors have conducted studies to show that residual personal data remains on the device after use of many popular apps. These studies include research on social networking apps such as Facebook, Twitter, and MySpace (Al Mutawa et al. 2012); cloud storage apps such as Dropbox, Box, SugarSync, and Syncplicity (Grispos et al. 2015); and general smart phone use (Glisson et al. 2011). One study (Grispos et al. 2014) put together residual artifacts resulting from the use of a variety of Google services and cloud-based synchronized apps to identify an individual's behavior patterns.

One exploratory analysis regarding health apps was conducted by (Campbell et al. 2015), and involved interviewing representatives from vendors of consumer grade biomedical devices. These vendors reported

similar concerning results, namely that data stored on the device was not encrypted, that vendors controlled remotely stored data, and that the remotely stored data was kept indefinitely. This study illustrated that vendors do not necessarily understand or protect the sensitive data in a manner consistent with the level of security and privacy offered by traditional electronic healthcare devices (Campbell et al. 2015).

Consistent with the perceptions of vendors of these services and devices, forensic analyses have revealed residual personal information on mHealth apps. Several authors have built taxonomies relating to the risk of these apps (Azfar et al. 2015; Grispos et al. 2013, 2014). The first authors created an initial taxonomy of mHealth apps. Ozdalga et al. (Ozdalga et al. 2012) grouped apps based on their primary purpose. These smartphone apps fell into four categories: patient care and monitoring; health apps for the layperson; communication, education, and research; and physician or student reference apps.

The next two studies built upon this categorical system to build and test taxonomies of risk (Azfar et al. 2015; Ozdalga et al. 2012; Plachkinova et al. 2015). Plachkinova et al. (Plachkinova et al. 2015) review the risks associated with mHealth apps, and built a risk model. The first dimension of the model was the app category, according to Ozdalga et al. (Ozdalga et al. 2012). The other two dimensions were threats and security risks. The threat categories relating to mHealth apps were identity threats, access threats, and disclosure threats. The security categories were composed of identity threats, such as the misuse of patient identity information; access threats, such as unauthorized access to PHI; and disclosure threats, such as unauthorized disclosure of PHI (Plachkinova et al. 2015).

Azfar et al. (Azfar et al. 2015) built on the work of the previous article by creating a taxonomy for mHealth apps based on the same categories also with actual residual data from the apps. This technical exploration uncovered numerous artifacts of different types. These artifacts were recovered during a forensic analysis of 40 mHealth apps on Android devices. The authors successfully recovered artifacts on the devices by the mHealth apps in the form of databases, user credentials, user personal details, user activities, user locations, activity timestamps, and images. The resulting taxonomy was composed of two dimensions, incorporating the categories of artifacts as one dimension, and the categories of mHealth as the other dimension.

A holistic categorical framework by Lewis and Wyatt (Lewis and Wyatt 2014) incorporates three separate dimensions to generate four categories for apps. These dimensions include a probability and severity risk assessment, the complexity of the app, and a list of contextual factors. This framework places apps into one of four broad categories of regulatory guidance based on an analysis of the three dimensions. The categories run from the lowest risk where the regulation is self-assessment, to the highest risk where the regulation falls under the FDA or other governing body.

Past research has shown that there is remains a regulatory gray area in the growing field of telehealth apps. The risks associated with end-user use of telehealth apps are currently not well understood. The majority of research has grouped all health-related apps together, under the umbrella term of mHealth. This grouping, while practical for creating taxonomies, does not capture or address HIPAA and FDA guidelines for covered apps. Specifically, three of the four categories of smartphone medical apps proposed by Ozdalga et al. (Ozdalga et al. 2012), are reference or personal use. These apps which function as health apps for reference, education, or for the layperson for personal tracking purposes, do not contain ePHI (Larson 2018; Plachkinova et al. 2015). The category of patient care or monitoring, including those apps for diagnosis and treatment of medical conditions, has received the least amount of attention from forensic research literature despite the greater risks from the presence of ePHI.

Given that some apps do leave residual data on devices and some apps do handle ePHI, we pose the following questions:

1) How much residual data remains on an android device as the result of the use of a telehealth app?
2) What components of this information directly violates HIPAA and how? Methodology

According to legislative guidelines and related works in mobile forensics, telehealth apps should be covered by various rules governing ePHI [7, 8, 13, 16, 33]. As such, our hypotheses are:

H1: Telehealth apps leave artifacts on android devices.

H2: The artifacts left after the use of a Telehealth app include legally protected ePHI.

To test the hypotheses, a forensic analysis on three apps was. The study consisted of a forensic analysis of an Android smart phone loaded with three Telehealth apps. The process was broken into four stages, which include: 1) preparing the smartphone device and installing the health app; 2) loading a data set into the application; 3) process the device using the XRY forensic device to extract the files and artifacts from the resulting memory dumps; and 4) accessing the phone via a standard USB file transfer method. We utilized a Samsung SM-G920T Galaxy S6 LTE-A (carrier: T-Mobile, unlocked) with an operating system of Android 6.0.1 to perform our tests. Prior to performing the case study steps, a factory reset was performed on the phone to remove any extraneous, or user downloaded apps or residual data not related to the present study.

Three apps were selected from the Google Play store based on a variety of criteria. The criteria include a minimum of 100,000 downloads, a minimum of 4 out of 5-star rating, and a statement that the app is explicitly designed to allow communication with a doctor or other healthcare provider. These apps include Amwell: Doctor Visits 24/7; Doctor on Demand; and Free Doctor, Doctor Gratis. The technical details for each of the three apps are given in Table 1.

	Amwell: Doctor Visits 24/7	**Doctor on Demand**	**Free Doctor, Doctor Gratis**
Updated	3/30/2017	4/13/2017	3/11/2016
Version	9.4.1.005_01	3.12.11	4.1
Installs	>500,000	>500,000	>100,000
Required version	Android 4.0 and up	Android 4.1 and up	Android 4.0.3 and up
Rating out of 5 stars	4.1 stars	4.7 stars	4.1 stars
Number of Reviews	4,330	12,992	5,059
Publisher	American Well	Doctor On Demand, Inc	Health2i Private Limited
Category	Medical	Medical	Health & Fitness
HIPAA compliant	In the app description	In terms of service	In the app description
Accreditation	American Telemedicine Assoc.	None	None

Table 1. App Details

Each app was downloaded from the Google Play store onto the Android device one at a time. After installation, each app was opened, notifications were read, requested information was supplied, and provider communication requested. This process was completed for each app individually and independently prior to moving on to the next app. The test data involved different but analogous patient names, demographic data, and medical histories. Using data sets that were comparable but different allowed for easier identification of recovered artifacts. Usage history and storage locations were documented for each app.

Two of the apps required an account to function, Amwell: Doctor Visits 24/7 and Doctor on Demand. No account was required for Free Doctor, Doctor Gratis. The next step was to request an appointment or communication with a healthcare provider. Test data was supplied to each of the apps, including at minimum an email address and basic demographic information such as name and reason for visit.

The first app installed was Amwell: Doctor Visits 24/7. Upon installing the app and opening it the first time, the user has the choice of logging in or signing up, and cannot proceed without an account. Required information includes: first and last name, date of birth (DOB), gender, location, email address, password, and optionally a service key and health plan. The next screen was titled 'My Services,' where the selection for medical was made. Appointments cost $59 and were with board certified doctors. Options available were to visit now or schedule an appointment. Phone number was necessary to book an appointment, and was input. Under visit now, the 'Get Started,' option was selected, followed by the requirement for a phone number. The next screen was for selecting the nature of the appointment. The following screens gave options for pharmacy, preexisting conditions, medical allergies, and vital signs. The vital signs included blood pressure, temperature, weight, and then an option to share this information. Insurance information was requested, along with payment information. The option to send a message with a photograph to the provider was selected, and a photograph was taken with the phone's camera through the app. The

message was not sent. After all information was completed, the appointment was requested. Finally, the app was logged out, without completing the appointment, closed, and the device restarted.

The Doctor on Demand app procedure was virtually the same as the first procedure, with minor variations in the order of requested information. Any differences in procedure were due to specific options and menu order within the app itself. The Doctor on Demand app did require an account for use, which involved almost identical demographic data to the Amwell app account creation. This information included first name and last name, DOB, phone number, address, insurance company name, insurance policy number, insurance group number, and pharmacy. An appointment was requested. When requesting the appointment, the following information was provided: reason for visit, current medications, allergies, current symptoms, other conditions, and payment information. After all information was completed, the appointment was requested. Finally, the app was logged out, without completing the appointment. The app was then logged out and closed, and the phone was restarted.

The Free Doctor, Doctor Gratis app procedure was significantly different from the other two apps due to differences in the app itself. This app did not require an account. Upon opening the app, the user was presented instead with advertisements and general health information. There was an option to chat with a medical health professional. Upon clicking on the chat option, a menu with options for the nature of chat included general health, diabetes, women's health, baby and infant, children's health, pregnancy, skin health, and men's health. One of these options was selected; however, there was a notification indicating that a doctor was not currently available. There was an option to input an email address to be contacted when a doctor became available. Upon putting in an email address, an error message prevented the user from completing the request. The error message indicated that there were required fields left blank; however, there were no additional fields visible. There was a link to the paid version of the app. The app was closed and the phone restarted.

After all apps were loaded with test data, a full extraction was conducted. The phone was put into developer mode through the settings menu by tapping on the version seven times, and USB debugging was turned on through the developer setting menu. The phone was then connected to the XRY, and a logical extraction was conducted. Backup was then selected to obtain third party app data. This process created a forensic copy of the files on the device for processing and analysis. A second extraction with the agent option for system apps was also conducted however it did not return relevant results. The phone was unplugged from the XRY and restarted.

The final step was to conduct a manual, standard file transfer to access user files from the phone. The phone was connected to a computer with a USB cable. Once the phone was connected, the phone notification appeared, for which the option to use the USB for file transfer was selected. A file transfer window opened on the computer, where files could be selected for transfer. All available files were transferred for review. The folders were reviewed to confirm files from the three apps of interest, along with possibly related media files, were present. The device was then ejected and unplugged from the USB and the phone was powered off.

Results

Data was successfully retrieved from all three apps on the phone. The original XRY extraction produced over 7,000 artifacts, although many of these were unrelated to the apps of interest. Two of these apps had data in plain text, the Doctor on Demand and Free Doctor, Doctor Gratis apps. The third app, Amwell: Doctor Visits 24/7 used a combination of encryption and server-side storage and did not have any identifiable information on the phone from the XRY retrieval. In total, 210 artifacts were recovered from the three apps. The aggregate results of the data collection are in Table 2. These results include only those artifacts readily identifiable as associated with the apps of interest, and do not include all artifacts retrieved from the phone.

The Amwell: Doctor Visits 24/7 app had the least amount of recoverable information. There were no evident files relating to this app, although there were multiple encrypted files. Breaking encryption and recovering data from encrypted files is out of scope of this research. The single interesting file to note

from Amwell: Doctor Visits 24/7 is that a photograph taken through the app was stored in the phone's default media storage folder.

	Amwell: Doctor Visits 24/7	Doctor on Demand	Free Doctor, Doctor Gratis
Cookies	0	4	12
Databases	0	4	6
Documents	0	18	5
Unrecognized	0	54	34
Cache*	10	0	63
Total	10	80	120

Table 2. File count from XRY extraction

The Doctor on Demand app had a wealth of artifacts and information stored on the phone. This app stored several Extensible Markup Language (XML) files, including information regarding the patient preferences and account information in plain text, for example see Figure 1. Additionally, there were several files which stored various account related activity that were missing the file extension information and thus could not be identified or opened. These files included in their name and file path information such as current employer, insurance, address, allergies, medications, credit card, pharmacy, and appointment scheduling information.

The Free Doctor, Doctor Gratis app had the largest number of artifacts recovered, although this app had the least patient information. There were 63 cache files from this app that were image files of the various advertisements and health information articles.

Analysis and Discussion

According to the HIPAA Privacy Rule (Goldstein and Pewen 2013), ePHI is any individually identifiable health information in electronic form. This information must be held by a doctor, insurance company, business associate, or other covered entity, and must relate to an individual's medical care. The ePHI rules include information transmitted over any electronic medium. These rules include demographic and generic information that is used or transmitted for the purposes of providing healthcare.

The data recovered from two of the three apps contained potentially harmful information about the user. This data was stored without encryption on the phone and ranged from demographic information to medical information. The data collected was further examined in the context of HIPAA and patient privacy. All three apps indicated from either their Google Play listing or terms of service that they are HIPAA compliant, although they did not include a specified BAA.

While all three apps claim to be HIPAA compliant, only the first app, Amwell: Doctor Visits 24/7, appeared to completely comply with the standards of security necessary for the storing and transmission of ePHI. While encryption in particular is not necessary to protect the data, however, the data should be protected in some way to prevent accidental or inappropriate disclosures [7, 13]. The worst offender for protecting patient information was the Doctor on Demand app. Figure 1 shows the XML text for the user data file com.android.doctorondemand.xml. This file contains personal health data such as current medications, insurance number, full address, symptoms, and more in plain text. This file also shows personally identifiable demographic data such as name, address, and phone number.

While sensitive information from the Free Doctor, Doctor Gratis app was not found, the app itself did not comply with HIPAA standards. The app did not request the same level of user information as the other two apps. Despite the lack of account creation initially, this app, was possibly less private and secure than the other two. When attempting to contact a healthcare provider, the app showed a long disclaimer. The app initially stated it was HIPAA compliant in the app's description, but this disclaimer states that the app is not. The disclaimer includes a warning that any information asked on the app can be visible to the public via a health-based social media site. The contradiction between the app's store description and the disclaimer can lead to false expectations of privacy by the user and confusion about the app's purpose.

Figure 1. XML file with patient information

In addition to the disclaimer, the app itself was not well secured. The user's email address was recovered, as were the databases where communications would have been stored if the user had successfully connected with a healthcare provider. Additionally, the questions posted through the app may also appear on a social networking healthcare website. This site is on the open Internet and does not require an account to view the questions and responses.

Conclusion

There are several issues with the regulatory landscape relating to healthcare apps. The first problem is that the guidelines are being written by different governing agencies with different motivations. These guidelines do not always line up with one another, creating gaps and conflicts. The second problem relates to roles. Vendors, healthcare providers, business associates, and patients all have differing responsibilities, and not all of them are covered under HIPAA and related regulations (Goldstein and Pewen 2013). These different roles can lead to confusion regarding whose responsibility is to protect ePHI, and how that role can be enforced.

The results of the case study portion illustrate the vast differences in how patient information is being handled and stored. Our examination of these apps support the first hypothesis. All the apps left some residual data on the phone. The second hypothesis is less clearly supported. The first app, Amwell: Doctor Visits 24/7, does not support the hypothesis that residual ePHI exists from usage of the app. The second and third apps, however, do support this hypothesis. Patient information, including ePHI, was found.

The case studies demonstrate the need for clearer regulatory guidance in healthcare-based apps. While the most detailed information was found from the Doctor on Demand app, it was the Free Doctor, Doctor Gratis app which is the most significant example of the privacy issues with unregulated telehealth apps.

Limitations of this study include using a small number of apps, using only one device, and using only free to download apps. Finally, the case study was conducted without completing an appointment with a healthcare provider. This step was skipped for several reasons. The first of which was to try to remain as closely within the terms of service and acceptable use as possible. The second reason was to avoid an unethical scenario wherein the researchers gave false information to a provider.

In the future, this work will be expanded to include additional apps and devices, such as iOS and android-based tablets. Additional Telehealth and Telemedicine apps will be investigated including those which connect or interface directly to medical devices.

References

Al Mutawa, N., Baggili, I., and Marrington, A. 2012. "Forensic Analysis of Social Networking Applications on Mobile Devices," *Digital Investigation* (9), The Proceedings of the Twelfth Annual DFRWS Conference, pp. S24–S33. (https://doi.org/10.1016/j.diin.2012.05.007).

Ali, E. E., Chew, L., and Yap, K. Y.-L. 2016. "Evolution and Current Status of Mhealth Research: A Systematic Review," *BMJ Innovations* (2:1), pp. 33–40. (https://doi.org/10.1136/bmjinnov-2015-000096).

Allen, C., Des Jardins, T. R., Heider, A., Lyman, K. A., McWilliams, L., Rein, A. L., Schachter, A. A., Singh, R., Sorondo, B., Topper, J., and Turske, S. A. 2014. "Data Governance and Data Sharing Agreements for Community-Wide Health Information Exchange: Lessons from the Beacon Communities," *EGEMS* (2:1). (https://doi.org/10.13063/2327-9214.1057).

Azfar, A., Choo, K.-K. R., and Liu, L. 2015. "Forensic Taxonomy of Popular Android MHealth Apps," *ArXiv:1505.02905 [Cs]*. (http://arxiv.org/abs/1505.02905).

Barmpatsalou, K., Damopoulos, D., Kambourakis, G., and Katos, V. 2013. "A Critical Review of 7 Years of Mobile Device Forensics," *Digital Investigation* (10:4), pp. 323–349. (https://doi.org/10.1016/j.diin.2013.10.003).

Campbell, M., Glisson, W., Loeser, D., Campbell, A., (2015). "Have We Left The Barn Door Open? An exploratory examination of data security in consumer grade bio-monitoring devices." Proceedings of the 2015 Conference of the Southeast Decision Sciences Institute.

Carroll, J. K., Moorhead, A., Bond, R., LeBlanc, W. G., Petrella, R. J., and Fiscella, K. 2017. "Who Uses Mobile Phone Health Apps and Does Use Matter? A Secondary Data Analytics Approach," *Journal of Medical Internet Research* (19:4), p. e125. (https://doi.org/10.2196/jmir.5604).

Colorafi, K., and Bailey, B. 2016. "It's Time for Innovation in the Health Insurance Portability and Accountability Act (HIPAA)," *JMIR Medical Informatics* (4:4). (https://doi.org/10.2196/medinform.6372).

Dinesen, B., Nonnecke, B., Lindeman, D., Toft, E., Kidholm, K., Jethwani, K., Young, H. M., Spindler, H., Oestergaard, C. U., Southard, J. A., Gutierrez, M., Anderson, N., Albert, N. M., Han, J. J., and Nesbitt, T. 2016. "Personalized Telehealth in the Future: A Global Research Agenda," *Journal of Medical Internet Research* (18:3). (https://doi.org/10.2196/jmir.5257).

Dorsey, E. R., and Topol, E. J. 2016. "State of Telehealth," *New England Journal of Medicine* (375:2), pp. 154–161. (https://doi.org/10.1056/NEJMra1601705).

Glisson, W. B., Storer, T., Mayall, G., Moug, I., and Grispos, G. 2011. "Electronic Retention: What Does Your Mobile Phone Reveal about You?," *International Journal of Information Security* (10:6), p. 337. (https://doi.org/10.1007/s10207-011-0144-3).

Goldstein, M. M., and Pewen, W. F. 2013. "The HIPAA Omnibus Rule: Implications for Public Health Policy and Practice," *Public Health Reports* (128:6), pp. 554–558.

Grispos, G., Glisson, W. B., Pardue, J. H., and Dickson, M. 2014. "Identifying User Behavior from Residual Data in Cloud-Based Synchronized Apps," *ArXiv:1411.2132 [Cs]*. (http://arxiv.org/abs/1411.2132).

Grispos, G., Glisson, W. B., and Storer, T. 2013. "Using Smartphones as a Proxy for Forensic Evidence Contained in Cloud Storage Services," in *2013 46th Hawaii International Conference on System Sciences*, , January, pp. 4910–4919. (https://doi.org/10.1109/HICSS.2013.592).

Grispos, G., Glisson, W. B., and Storer, T. 2015. "Recovering Residual Forensic Data from Smartphone Interactions with Cloud Storage Providers," *ArXiv:1506.02268 [Cs]*, pp. 347–382. (https://doi.org/10.1016/B978-0-12-801595-7.00016-1).

Larson, R. S. 2018. "A Path to Better-Quality MHealth Apps," *JMIR MHealth and UHealth* (6:7). (https://doi.org/10.2196/10414).

Lateef, F. 2011. "The Practice of Telemedicine: Medicolegal and Ethical Issues," *Ethics & Medicine* (27:1), p. 17.

Lee, V. S., Miller, T., Daniels, C., Paine, M., Gresh, B., and Betz, A. L. 2016. "Creating the Exceptional Patient Experience in One Academic Health System," *Academic Medicine* (91:3), p. 338. (https://doi.org/10.1097/ACM.0000000000001007).

Lewis, T. L., and Wyatt, J. C. 2014. "MHealth and Mobile Medical Apps: A Framework to Assess Risk and Promote Safer Use," *Journal of Medical Internet Research* (16:9), p. e210. (https://doi.org/10.2196/jmir.3133).

Marcoux, R. M., and Vogenberg, F. R. 2016. "Telehealth: Applications From a Legal and Regulatory Perspective," *Pharmacy and Therapeutics* (41:9), pp. 567–570.

Ozdalga, E., Ozdalga, A., and Ahuja, N. 2012. "The Smartphone in Medicine: A Review of Current and Potential Use among Physicians and Students," *Journal of Medical Internet Research* (14:5), p. e128. (https://doi.org/10.2196/jmir.1994).

Plachkinova, M., Andrés, S., and Chatterjee, S. 2015. "A Taxonomy of MHealth Apps – Security and Privacy Concerns," in *2015 48th Hawaii International Conference on System Sciences*, , January, pp. 3187–3196. (https://doi.org/10.1109/HICSS.2015.385).

Saleem, Y., Taylor, M. H., and Khalifa, N. 2008. "Forensic Telepsychiatry in the United Kingdom," *Behavioral Sciences & the Law* (26:3), pp. 333–344. (https://doi.org/10.1002/bsl.810).

Sood, S., Mbarika, V., Jugoo, S., Dookhy, R., Doarn, C. R., Prakash, N., and Merrell, R. C. 2007. "What Is Telemedicine? A Collection of 104 Peer-Reviewed Perspectives and Theoretical Underpinnings," *Telemedicine and E-Health* (13:5), pp. 573–590. (https://doi.org/10.1089/tmj.2006.0073).

Thilakanathan, D., Calvo, R. A., Chen, S., Nepal, S., and Glozier, N. 2016. "Facilitating Secure Sharing of Personal Health Data in the Cloud," *JMIR Medical Informatics* (4:2). (https://doi.org/10.2196/medinform.4756).

Washington, V., DeSalvo, K., Mostashari, F., and Blumenthal, D. 2017. "The HITECH Era and the Path Forward," *New England Journal of Medicine* (377:10), pp. 904–906. (https://doi.org/10.1056/NEJMp1703370).