Mobile Networks and Applications (2023) 28:1282–1292
https://doi.org/10.1007/s11036-022-02049-8

Sickly Apps: A Forensic Analysis of Medical Device Smartphone Applications on Android and iOS Devices

George Grispos[1] · Kim-Kwang Raymond Choo[2] · William Bradley Glisson[3]

Accepted: 13 December 2021 / Published online: 22 October 2022

Abstract
Smartphone devices are increasingly being integrated into a variety of medical settings. An emerging trend is the development of smartphone applications that interact with medical devices connected to the Internet. While this fusion of technology can provide various benefits for both patients and medical professionals, there are concerns that these devices could become targets for cybercriminals. Therefore, a digital forensic investigation of these medical devices could be needed. However, researchers have suggested that the investigation of medical devices is unlikely to be straightforward, and that conventional forensic evidence acquisition might not be possible. Hence, this paper proposes that smartphone applications, which interact with medical devices, could provide an alternative source of digital evidence when investigating the device itself. The research contribution is twofold. First, the paper presents an empirical investigation to using residual data recovered from medical smartphone applications, as a means for forensically examining medical devices. Second, the paper documents the forensic artifacts that are generated by specific medical device smartphone applications on Android and iOS smartphones.

Keywords Medical device · Smartphone · Application · Digital forensics

1 Introduction

Mobile devices (including smartphones) are increasingly being integrated into a variety of medical settings. According to a 2020 survey [3] by the American Medical Association, nearly 90% of surveyed medical professionals reported using digital health tools, including mobile devices, during patient interaction. The implementation and use of mobile devices can play a significant role when attempting to provide healthcare services to patients remotely, allowing patients to seek medical advice without visiting a medical professional [5]. Further complicating matters, many individuals are now choosing to use mobile medical services and applications within their own home [15, 17, 36]. These individuals are using medical smartphones applications and services for a variety of purposes, including illness and medication management, remote reporting of medical information, and even medical emergencies. However, while the benefits of integrating these technologies into medical settings are clear, the accumulation of medical information on mobile devices and applications has created a number of opportunities for cybercriminals to exploit [38].

For example, according to a Verizon industry report [45] nearly 25% of healthcare organizations suffered a mobile–related data breach, with 67% of these organizations classifying this breach as a "major" incident within their organization. In fact, government agencies in the United States have published warnings that medical devices connected to the Internet, along with their applications are increasingly likely to be targeted by cybercriminals [41, 44]. These concerns recently became a reality when a team of cybersecurity researchers discovered an unprotected database on the Internet containing tens of millions of medical device and application records, belonging to people from a diverse number of countries [13].

Hence, the security and privacy of patient and medical device data has become a concern for the cybersecurity

✉ George Grispos
ggrispos@unomaha.edu

Kim-Kwang Raymond Choo
raymond.choo@fulbrightmail.org

William Bradley Glisson
glisson@latech.edu

[1] University of Nebraska at Omaha, Omaha NE, USA

[2] University of Texas at San Antonio, San Antonio, TX, USA

[3] Louisiana Tech University, Ruston, LA, USA

community. In line with this thought, medical regulators in both the United States [39] and Australia [4] have released cybersecurity guidelines concerning medical devices. More specifically, the FDA guidelines recommend that medical device and application developers "address cybersecurity throughout the product life–cycle, including during the design, development, production, distribution, deployment and maintenance of the device" [39]. The same FDA guidelines go on to state that device manufacturers should also incorporate mechanisms that allow the capture of forensically-sound evidence from medical devices.

When cybersecurity incidents impacting medical devices occur, one response from a healthcare organization is to conduct a digital forensic investigation [18, 30]. The purpose of such an investigation is to identify any potential loss of patient information, as well as attempting to identify who or what was responsible for the incident [15]. However, the forensic investigation of medical devices is expected to be difficult [15]. One of the primary difficulties foreseen is the acquisition and collection of medical data, in a manner such that it can accepted as evidence into court proceedings. One reason for these difficulties is that many traditional forensic tools support the collection of data from storage media, such as hard disk drives, which might not be available in many medical devices [18].

Recent years has seen the emergence of a technological trend that involves smartphone applications being developed to provide Internet access for various medical devices [12, 17]. Many of these devices (e.g., the KardiaMobile [1]) have received FDA clearance and can be used in hospitals, other medical environments, and even private homes. Previous research [19, 34] has established that smartphone applications produce residual data, which could be used to forensically investigate environments, such as cloud computing. This information provided the idea that smartphone applications that communicate with medical devices could also provide investigators with residual data for forensic investigations. Hence, the hypothesis that directed this research is: *medical device smartphone applications can be used by a forensic investigator as a source of potential digital evidence, when investigating a corresponding medical device*. This hypothesis resulted in the following research questions:

1. What user metadata can be retrieved from a smartphone that interacts with a corresponding medical device?
2. What medical device usage metadata can be retrieved from a smartphone that interacts with a corresponding medical device?
3. What other forensically–relevant artifacts are generated by a medical device smartphone application that interacts with a medical device?

This research enhances and develops concepts presented in prior conference publications [16, 17]. This paper extends the initial studies through an extended literature review, the examination of additional medical devices, and the introduction of an additional smartphone operating system. Relevant information and data from the initial conference publications are included in this journal publication for completeness. The research contribution is twofold. First, the paper presents an empirical investigation to using residual data recovered from medical smartphone applications, as a means for forensically examining medical devices. Second, the paper documents the forensic artifacts that are generated by medical device smartphone applications on Android and iOS smartphones. The balance of this paper is as follows: Section 2 examines published research on forensic investigations of medical devices and the forensic investigation of mobile phone applications. Section 3 presents the methodology used in this research, while Section 4 presents an analysis of the results, discusses the findings and limitations of the research conducted. Section 5 draws conclusions and presents future work.

2 Previous Work

Digital forensics concerns the investigation of data collected regarding a suspected cybercrime or security incident [31]. The objectives of a digital forensics investigation is to allow an investigator to answer five questions: what, why, who, when, and where [14]. An analysis of the literature suggests that the digital forensic investigation of medical devices is a topic of concern for both industry [30] and academia [6, 9, 15, 24, 28].

Ellouze et al. [9] argue that the investigation of medical systems introduces four main challenges for forensic investigators. These include complications due to the large amount of potential evidence produced by medical devices, a lack of integrity and trustworthiness from medical device evidence, the problem of acquiring evidence from complex and interconnected medical systems, and the different types of evidence that could be recovered from medical systems. Ellouze et al. [9] go on to state that they expect two types of evidence to be recovered from medical devices, the first being information about the security of the device (e.g., authentication information and access logs), and the second being information related to the patient's medical status. With much of this information being collected and stored within Electronic Health Records (EHRs), Jahankhani and Ibarra [24] add that these records could also become a target for malicious actors and therefore investigators need to include such evidence from EHRs in their investigation of medical devices and networks.

Grispos and Bastola [15] focused their attention on discussing the potential value of digital evidence for the healthcare industry. They outline five situations where such evidence can help in a medical context: helping provide answers into suspicious deaths, the investigation of medical device cybercrime, investigating incidents of medical malpractice, using forensics to audit medical trials, and investigating abuse of medical technology connected to the Internet. As a result, Grispos and Bastola [15] present the argument that medical device data will increasingly appear in a variety of court proceedings. This argument is also made by Maras and Wandt [28], who go on to discuss the United States court case State of Ohio v. Compton, which involved the introduction of digital evidence from medical data generated by a pacemaker. Chernyshev et al. [6] focus their attention on data breaches that occur within Electronic Medical Records (EMRs), along with the forensic challenges that could occur investigating these breaches. The results of their analysis into various EMR systems is that they do not appear to log enough events to assist with the forensic investigation of incidents involving these systems. Hence, Chernyshev et al. [6] conclude that without these detailed logs, it might not be possible to support or refute potential hypotheses surrounding the incident involving an EMR system.

As a response to the above concerns, various solutions have been proposed in the literature. Ellouse et al. [10] propose a solution concerning the investigation of implantable medical devices and developed a number of approaches to assist investigators with the retrieval of potential evidence logs that could be used to explain medical events. Cusack and Kyaw [7] argue that as a result of recent hacking attempts, medical environments should not rely on security alone and that other incidents and cybercrimes can occur. As a result, Cusack and Kyaw [7] present a forensically–ready network architecture to support wireless devices in hospital environments. Liu et al. [26] propose a theoretical approach for handling digital investigation of medical devices connected to the Internet that includes taking into account the cyberspace, the social space, the physical space, and the psychological space, with respect to medical devices and systems. Grispos et al. [18] present a solution that involves the integration of forensics principles and concepts into the engineering of forensic–ready medical systems. While various solutions to forensically investigating medical devices have been proposed, one problem they do not address is the residual data generated by medical devices, nor how this data can be captured, analyzed or used for forensic investigations.

When medical devices are targeted by cybercriminals, any mobile devices (e.g., smartphones) that have interacted with these medical devices, could be subject to a mobile phone forensics examination. Mobile phone forensics is defined as "the science behind recovering digital evidence from mobile phones" [27]. Hence, the digital forensic community has dedicated much research to identifying and decoding artifacts that are generated by smartphone devices and the applications stored on these devices. Quick et al. [35] and Grispos et al. [19, 20] investigate the residual data generated by end–devices (including smartphones) and servers involved in public and private cloud storage services. Norouzizadeh et al. [32] focused their research efforts on social network applications, and demonstrated how a forensic investigator can recover a variety of data related to popular social networks including authentication credentials, messages, posts and user information, which can be used to assist in the forensic investigation of these applications. Dargahi et al. [8] analyzed three Android applications, Skype, WhatsApp and Viber and reported that messages, contact information, telephone details, and pictures could be recovered from these applications. Alyahya et al. [2] examined the artifacts generated by Snapchat, who demonstrated that it was possible to recover user metadata and messages, which were supposedly deleted by the individual using the Snapchat service. Maus et al. [29] identified that many geolocation datapoints exist on a smartphone and developed a software tool for collecting this geolocation information generated by various applications on Android devices. While previous research has presented various challenges to investigating medical devices and the forensic analysis of various smartphone applications, minimal research has investigated the ability to examine the residual data generated on the smartphone applications that have interfaced with a medical device.

3 Methodology

This research consists of a controlled experiment [33] (summarized in Fig. 1) using two smartphones and seven medical devices that interface with a smartphone application installed on the two smartphones. The two smartphones selected were a Samsung Galaxy, which executes the Android operating system, and an Apple iPhone that executes the iOS operating system. These two devices were selected because the underlying operating systems account for approximately 99% of the smartphone operating system market share [37]. These devices were also selected because they are supported by the mobile forensic toolkit (MSAB XRY) used in the experiment to extract and analyze the application data generated on the smartphones. While other smartphones could have been used, these two devices were selected based on their availability.

Seven medical devices were selected for the experiment and were obtained from three different manufacturers. These medical devices use a corresponding smartphone application. The medical devices were selected because they offer both an Android and iOS version of their respective application. These specific devices were used based on their

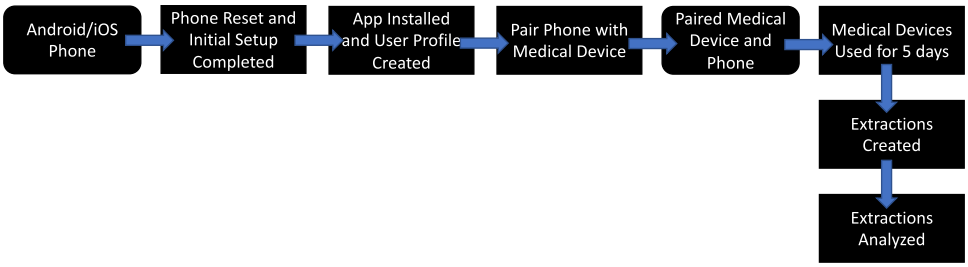

Fig. 1 Summary of controlled experiment

Table 1 Medical devices used in the experiment

Manufacturer	Device Name	Application
iHealth	HS6 Core Scale	iHealth MyVitals
iHealth	BP5 Feel Blood Pressure Monitor	iHealth MyVitals
iHealth	PO3M Air Pulse Oximeter	iHealth MyVitals
iHealth	BG5 Gluco-Monitoring System	iHealth Gluco-Smart
Nokia	Cardio Scale	Health Mate
Nokia	BPM+	Health Mate
Kardia	Mobile ECG Device	Kardia

availability for purchase in the United States. Table 1 provides an overview of these devices, along with the application that accompany the specific device.

Specific versions of the smartphone applications were used in the experiment. With regard to the iHealth MyVitals application, the Android version used was 3.7.1 and the iOS version was 3.7.2. The Android version of the iHealth Gluco-Smart was 4.5.3 and the iOS version of this application was 4.5.3. Regarding the Health Mate application, the Android version used was 3.5.4 and the iOS version used was 4.0.1. Finally, the Karida application included Android version 5.1.2 and iOS version 5.1.2. The medical devices make use of different mechanisms for transmitting information to its specific application. The Core and Cardio scales rely on Wi–Fi signals, the Kardia ECG device makes use of ultrasound signals to the smartphone's microphone, while the remaining devices use Bluetooth connections to receive and transmit information.

The controlled experiment consisted of four iterations, the first and second iteration focused on the medical devices that included the MyVitals and Gluco–Smart applications, while the third and fourth iterations involved the Health Mate and Kardia applications, respectively. The experiment consisted of the following steps:

1. The smartphones were returned to their factory settings, using instructions found in each device's manual.
2. A Google and Apple account were created using a separate desktop web browser, one account for each smartphone.
3. Each smartphone was powered–up and the device initialization was completed. The respective account created in the previous step was used to complete the setup of the device after the factory reset.
4. The Android and iOS smartphones were used to access the Internet using a dedicated network in order to download and install the medical device applications. After the installation of these applications, a new user profile was created using each application, for the purpose of the experiment. It must be noted that the information provided to create the user profile can be considered 'test information', and did not include any real–world personal information.
5. User credentials created in the previous step were then used to login into the application and each medical device application was 'paired' with its respective medical device, using information provided in the medical device manuals. A confirmation was received that each device was successfully paired with its accompanying smartphone application.
6. The first author then proceeded to use the medical devices and applications for five days. It must be noted that for the BG5 glucose monitor, instead of providing the device with a blood sample for each reading, the author used a solution consisting of water and sugar. Each medical device provided the results of the reading undertaken, which were documented together with the date and time.
7. Upon completion of the fifth day, both smartphones were subjected to the XRY toolkit, in order to produce extractions of each device's internal memory. Information provided by the XRY toolkit assisted in completing this process and the extraction of each device took approximately fifteen minutes.
8. The extractions produced in the above step were then loaded into XAMN, forensic software that accompanies the XRY toolkit. XAMN decoded the two smartphone filesystems, and different analysis techniques were used to examine the extractions in order to locate and recover artifacts produced by the medical device's application.

Fig. 2 Sample of Evidence from TB_SPo2Result Table

MechineDeviceID	MeasureTime	LastChangeTime	PhoneCreateTime	Result	PR	PI
Filter	Filter	Filter	Filter	Filter	Filter	Filter
5CF821DED2ED	1530884863	1530884878	1530884863	96	77	8.3
5CF821DED2ED	1530829549	1530829596	1530829549	97	89	9.69999

The above steps were repeated for each smartphone and medical device on both the Android and iOS applications.

4 Analysis

The examination and analysis of the medical device smartphone applications revealed that user identifiable information and medical device metadata can be recovered from the iHealth MyVitals, Health Mate, and Kardia applications. This information was recoverable from both the Android and iOS version of these applications. With regard to Gluco-Smart application, the iOS version stores user and device information in plaintext, but the Android version of the application makes use of encryption techniques to obscure many of the artifacts generated. However, it was still possible to recover some user–specific information from Extensible Markup Language (XML) files generated by the Android version of the application.

The following subsections document the user and medical device information that can be recovered from each of the smartphone applications, with respect to the test user and their interaction with the medical devices. All other artifacts recovered from the smartphone and other applications are considered out of scope.

4.1 Android Smartphone Applications

Previous literature has established that the Android filesystem, creates and stores user–generated data under the primary location `/data/data` [22]. All the Android smartphone applications created a folder with a different name under this location.

4.1.1 Android iHealth Devices

The iHealth MyVitals application creates a folder named `iHealthMyVitals.V2`, which contains artifacts related to the three iHealth devices included in the experiment. One of the main artifacts in this folder is a database named `androidNin.db`, which consists of several tables of interest to a forensic investigator:

- **TB_BPResult** can be used to recover blood pressure monitor readings, heart rate measurements, timestamp information, the device identifier, along with user–specific information such as the user account and any notes as entered by the user at the time of the recording.
- **TB_SPo2Result** can be used to recover pulse oximeter readings. Figure 2 highlights some of the information that can be found in this table including the heart rate (PR), perfusion index (PI), oxygen level (Result) and the time the reading was undertaken (MeasureTime).
- **TB_TemperatureHumidity** is a table related to the Core scale and contains metadata regarding humidity levels, and conditions such as how much light was in the room when the scale was used.
- **TB_WeightOnlineResult** describes the user's readings from the Core scale and includes information such as: weight, body mass index, body fat percentage, percentage of body water, muscle mass, daily calorie intake, and bone mass. The date and time of each scale reading can also be found in this table.
- **TB_Userinfo** contains metadata about the device user including their name, when they were born, the timezone they are located in, as well as the email address associated with their user account.

User and device metadata related to the iHealth MyVitals application is also recoverable from XML files. Metadata recovered from these files include the email address used to register for the iHealth services, the medical devices connected to the application, and network information. One interesting finding is the ability to recover the user's unencrypted authentication credentials (including their password, see Fig. 3) from a file called `sp_user_region_host_info.xml`. This can be combined with the user's email address to access the user's profile and other medical data stored within the iHealth service.

The Gluco-Smart application generates metadata in a folder called `jiuan.androidBg.start`. While several artifacts, including databases are visible in this application's folder, these artifacts are encrypted and can not be read without a password. Attempts to authenticate using the user's test password were unsuccessful. Moreover, an analysis of the smartphone extractions that contained the Gluco-Smart application did not reveal a password that could be used to decrypt the artifacts. One potential explanation is that the password itself is stored as a hash on the smartphone, and this can not be identified as a password. Further investigation is therefore needed to identify how to decrypted information from the Gluco-Smart application artifacts. While the

encrypted information could not be recovered, a file named `user_info.xml` was found unencrypted and appears to contain user metadata and device identifier information.

4.1.2 Android Kardia Device

With regard to the Kardia Mobile, a folder called `com.alivecor.aliveecg` is generated by the application in order to store various metadata about the Kardia device and the test user. ECG data can be recovered from a subfolder called `/files/ecgs`. Further analysis of these ECG files using a hex editor revealed that each file consists of timestamps of each recording, the type of smartphone involved in the recording, and the version of software currently applied to the Kardia device. Figure 4 provides an example of this analysis using a hex editor.

PDF documents visualizing the ECG recordings can also be retrieved from the `com.alivecor.aliveecg` folder. Information that is documented within these PDF files include the user's birthday, the timestamp of when the specific reading was taken, and the pulse rate, documented as beats per minute. The Kardia application also appears to store further user and device information in a database called `ECG.db`. Information that can be found in this database includes timestamps, ECG readings, user information, the user's birthday, height, weight and gender. The Kardia application also stores potential evidence in XML files, such as the user's birthday, email address information, and timestamp information related to the last recording using the Kardia device.

4.1.3 Android Nokia Devices

Android Nokia device artifacts were found in a folder called `com.withings.wiscale2`, which contains a database called `withings-WiScale.db`. While this database consists of many tables, only three contain evidence of interest to this experiment. The `devices` table, (Fig. 5) contains metadata about the medical device itself, including network information, timestamps, device type and usage, as well as battery levels.

A table named `measure` appears to describe the user's interactions with the Cardio scale and BPM+ devices. Various metadata about these interactions (e.g., readings) can be recovered from this table, including timestamp information, pulse rates, systolic, and diastolic values, weight and body fat information, bone and muscle mass, and body index values. The final table of interest is called `users`, and describes user–specific metadata such as the forename and surname, the user's gender, birthday and email address information.

Fig. 3 Unencrypted Password Found in XML File

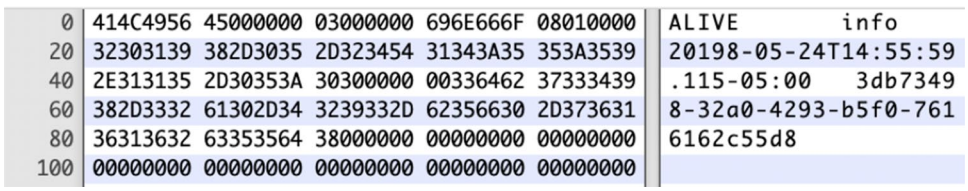

Fig. 4 ECG File Analysis Using a Hex Editor

id	associationDate	lastUseDate	modifiedDate	macAddress
Filter	Filter	Filter	Filter	Filter
5595648	1541806236000	1542127729662	1542127635000	00:24:e4:5a:ee:6c
5402710	1541806407000	1542070868000	1542093243000	00:24:e4:57:12:c4

Fig. 5 Sample of Evidence from *Device* Table

4.2 iOS Applications

The iOS applications create a folder under the path `/private/var/mobile/containers/data/application` [23]. User metadata and device readings were recovered from each application's folder under this path.

4.2.1 iOS iHealth Devices

Artifacts related to the iHealth scale, blood pressure monitor and oximeter were recovered from folder called `com.ihealthlabs.ihealth`. An important artifact in this folder is a database called `ihealth.sqlite`. This database contains six tables of interest to a forensic investigator. The following information can be found in these tables:

- **ZUSER** can be used to recover the user's birthday, height, weight, email address, and location.
- **ZSCALETEMPRHINFO** can be used to recover room conditions such as the temperature and humidity levels and timestamp information.
- **ZSCALEMEASUREMENT** describes the user's weight reading, body mass index, percentage of body fat, body water, muscle mass, daily calorie intake, bone mass, along with timestamp information.
- **ZBPMEASURERESULT** describes blood pressure values, pulse rate during the reading, timestamp information, any text notes documented after the recording, along with the timestamp of when these notes were created.
- **ZOXMEASURERESULT** describes the recorded oxygen level and pulse rate, perfusion index, timestamp information when the reading took place, and timestamps when any notes were created.
- **ZACCESSORYCONNECTLOG** contains metadata about the device including device names, type, firmware and hardware versions, model number, and device serial numbers.

In addition to retrieving the above information, similar to the Android application, the user's password was recovered in plaintext. The Gluco-monitoring application creates a folder called `com.ihealthlabs.BG`. In this folder, user and device metadata is stored in a database called `ihealth.sqlite`. Data that can be recovered includes the user's name and birthday, the user's height, weight and gender, and the user name and email address used to access the iHealth service.

4.2.2 iOS Kardia Devices

The iOS Kardia application generates a folder called `com.alivecor.professional.aliveecg` that is used to store user and device metadata. The primary location of the artifacts generated by the Karida Mobile application is a database called `AliveECGDB.sqlite`. Three tables contain relevant forensic information:

- **ZKDMBLOODPRESSURERECORDING** can be used to recover blood pressure values, the day and time when the blood pressure reading was undertaken, transcripts documented at the time of the reading and pulse rate information.
- **ZKDMWEIGHT** can be used to recover the user's height, weight, and timestamp information.
- **ZECG** contains timestamps when ECG readings were taken, results of ECG readings, duration of ECG readings, patient's forename, surname, gender, and birthday information.

In addition to the database and associated tables, PDF and ECG files were also recovered from the parent folder of the Kardia application. The file headers for ECG files generated by the iOS application are in the same format to those identified in the Android version of the application. The Kardia applications also store information in a Property List (plist) file called `alivecor.professional.aliveecg.plist`. Information that can be recovered from this plist file includes the user's forename and surname, the user's gender and birthday, as well as the email address used to register the user's profile account.

4.2.3 iOS Nokia Devices

The Nokia Cardio and BPM+ devices store metadata in a folder called `com.withings.wiScaleNG`. Within this folder are two databases that contain various metadata related to the Nokia devices. The first database is called `associated_device.sqlite` and consists of metadata about the two devices and their interaction with their respective smartphone applications, including: the name/type of the medical device, battery states, the firmware installed on the device, MAC addresses, and the last known connection time. The second database is called `ID_Measure.sqlite` and contains the user's readings with the two Nokia devices. Information that can be found in this database include every measurement taken with the Cardio and BPM+ devices and timestamp information.

In addition to the database files, logs were identified in the `com.withings.wiScaleNG` folder that contain device and user information. These log files describe 'transactions' between the two Nokia devices and their accompanying

smartphone applications. Other information that can be recovered from the log files include MAC address information, smartphone application version numbers, timestamp information and pairing information between the application and Nokia devices. Moreover, the analysis of the log files revealed that it was also possible to recover the user's email address, timezone, last known IP address, and the devices that have interfaced with the smartphone application.

4.3 Implications of Findings

An analysis of the experimental findings suggest that these results could have a range of implications for both the digital forensics and medical communities. However, there is the potential that the research results can also help both communities, in particular during the undertaking of 'cyber autopsies'. Grispos and Bastola [15] define a cyber autopsy as "the digital forensic examination of medical devices, which have medically supported or interacted with a patient either at home or within a hospital setting". As this definition encompasses all medical devices that have interacted with a patient [21], it can include various smartphone applications that have collected data from a medical device or have been entered by the user in their own home.

One particular context where the residual data from the medical device smartphone applications could be of use is during a cyber autopsy into an individual's death that has raised questions and a traditional autopsy is required. The results from a medical study [25] conducted between 2012 and 2017 involving pathological autopsies, revealed that the time of death could not be established in 27% of the cases and that the manner of death could not be established in 34% of the cases, using traditional autopsy techniques and data. These medical researchers went on to suggest that the examination of personal cardiac implantable electronic devices could help provide answers to these suspicious deaths [25]. While the analysis of implantable devices could assist forensic pathologists with more information into the circumstances surrounding an individuals death, not every suspicious death could include the patient wearing an implantable device. Hence, alternative sources that could provide a forensic pathologist with more information could include medical devices and applications such as those evaluated in this research. The results from the experiment have shown that most of the applications include timestamp information concerning device use, as well as readings concerning blood pressure and electrocardiograms. These two types of readings, along with the date and time of the readings can help provide a pathologist with a better picture of a deceased individual's medical state, prior to their death. Moreover, this information could actually help identify the cause of death should the data from the devices indicate an abnormality. It is interesting to note that the Lacour et al. [25] study confirmed that some of the cardiac implantable electronic devices had to be examined by the device manufacturers, which suggests digital forensic domain experts are needed to help forensic pathologists. Hence, we envisage forensic pathologists working together with digital forensic experts to select devices of interest and then implementing appropriate digital forensic tools and techniques to collect, recover and decode artifacts from the selected medical devices.

As further cyber autopsies are conducted, there is the potential that data from medical devices will find its way into criminal and civil litigation cases, as digital evidence. As noted by Maras and Wandt [28], this will not be without resistance from individuals who do not want this information entering the judicial system. While the issue of an individual's rights concerning their medical information being used against them is out of scope for this paper, using the data from the smartphone applications could enhance the general admissibility of the data as evidence. The tools and processes of extracting and analyzing mobile phone data have largely been accepted by the courts as acceptable approaches [19]. As this experiment has shown, the same tools and processes can be used to extract potential evidence from smartphone applications that accompany medical devices. Hence, the approach used in the experiment provides a solution to an emerging problem, using existing tools and processes that have been accepted by the judicial system to collect and retrieve data from medical devices.

While the focus of the paper as been the investigation of medical devices using smartphone application data, it must be acknowledged that the experimental results have also highlighted potential security and privacy concerns. In 1996, the United States passed into law the Health Insurance Portability and Accountability Act (HIPAA). This states that healthcare organizations should "maintain appropriate administrative, technical, and physical safeguards for protecting electronic patient health information" and "preserve the confidentiality, integrity, and availability of collected (electronic patient health information) data, as well as protecting against malicious users and unauthorized disclosures" [43]. However, the research findings suggest that all the evaluated applications, with the exception of the Android iHealth Gluco-Smart application, are putting a user's information at risk, from a HIPAA perspective. Unencrypted identifiers such as forename and surname, birthday and gender, as well as medical information such as blood pressure and ECG device readings were found in various locations on the smartphone file–system. Complicating matters even further is the potential to access a user's account using unencrypted authentication credentials that could allow a malicious actor to obtain other medical information that might not be present on the smartphone, but be stored in a health provider's cloud service. Hence, it could be argued that there is data leakage from the unencrypted

smartphone applications evaluated in the experiment and that potential security and privacy liabilities could emerge when smartphone devices containing this information are either misplaced or stolen.

Moreover, the medical devices included in the experiment all appear to have obtained 510(k) clearance from the Food and Drug Administration (FDA), which demonstrates that the device is "as safe and effective, that is, substantially equivalent, to a legally marketed device" [40]. However, a deeper analysis of the 510(k) documents revealed that none of the documents discussed or introduce the fact that the devices include an accompanying smartphone that will store user and device information, in plaintext, on an interacting smartphone. Further analysis of other FDA documentation [42] also provides detailed recommendations to medical device manufacturers, but it does not discuss the implications of residual data generated by smartphone applications, that interact with FDA–cleared medical devices. Hence, this research has highlighted a potential gap in the healthcare industry with regard to further guidelines and potential medical device security and privacy requirements from the FDA and other regulators outside the United States, for example the European Union's (EU) General Data Protection Regulation (GDPR).

In fact, GDPR legislation requires that mobile application developers integrate privacy–by-design features (e.g., encryption) in order to safeguard a user's privacy [11]. While the applications evaluated in the experiment collect user personal data according to GDPR (such as login details), only one out of the four medical device applications made use of encryption to protect this information. However, the applications included in this research were downloaded from application stores intended for users from the United States and not in the EU. Hence, further investigation is needed to identify if the "EU versions" of the four applications contain privacy–by-design features and to what extent these features have been integrated in the mobile application architectures [11].

4.4 Study Limitations

The research presented in this paper is limited in the following ways. The experiments were undertaken using smartphones and medical devices procured in the United States (U.S.). The smartphones contain network software specific for mobile phone providers in the U.S., while the medical devices were bought from the U.S. version of the manufacturer's website. The experiment was only executed once on each smartphone, due to time restrictions and the experiment focused on specific versions of the smartphone operating systems. While a physical extraction was used for the Android smartphone, only a logical extraction was possible on the iOS smartphone. Finally, the experiment utilized test information, as opposed to using the devices in real–world settings, in order to populate the applications.

4.5 Summary of Results

The experimental results have shown that smartphone applications that accompany medical devices contain user–specific and medical device information. The user–specific information that can be recovered includes forenames and surnames, a user's birthday and gender. From the perspective of medical information, various different medical data points were identified from the smartphone applications including weight and height data, pulse rate information, blood pressure readings (systolic and diastolic values), oxygen level readings, weight information (e.g., bone mass, body fat readings, body mass index values), ECG readings, and timestamps.

Overall, the analysis of the experiment results support the hypothesis, medical device smartphone applications *can* be used by a forensic investigator as a source of potential digital evidence, when investigating a corresponding medical device. While this statement does not hold for the Glucosmart application, it does hold for the other three smartphone applications evaluated on both smartphones. Potential user data that can be recovered from the medical device smartphone applications include forename and surname, birthdays, gender information and email addresses, while medical device data recovered includes heart rates, blood pressure readings, and ECG readings. Moreover, other artifacts that were recovered include unencrypted usernames, passwords and authentication tokens.

5 Conclusions and Future Research

Mobile devices, such as smartphones, are increasingly being used in a variety of medical settings, including hospitals and private homes. As a result, medical information is beginning to accumulate on these devices that is making them an attractive target for cybercriminals. Hence, it is realistic to assume that digital forensic investigations involving a medical device will likely include smartphones and other mobile devices that have interacted with the medical device itself. The results show that medical device smartphone applications can be used by forensic investigator as a source of potential digital evidence, when investigating a corresponding medical device. This evidence could assist with the investigation of cybercrimes or security incidents against a medical device. The approach evaluated in this research provides one solution for addressing the limited number of tools and techniques for investigating medical devices, provided the device interacts with an accompanying smartphone application.

Future research includes extending this research to other medical devices from a variety of manufacturers in order to evaluate if the hypothesis will hold for applications running on different smartphone operating systems. Further research is also needed to examine medical devices themselves, including the development of process and tools to assist in this endeavor. A comparison could be made between data sets obtained from the medical device, with those obtained in this paper. *Does examining the medical device present a larger or smaller dataset of potential evidence?* The answer to this question can assist healthcare organizations develop decommissioning plans and procedures once they have chosen to stop using a particular device and do not want medical or private user information from leaking to the wider public. Finally, future research will also investigate the application of machine learning algorithms to develop detailed medical profiles. The idea behind this research is to investigate if it is possible to connect a specific individual to a device, based on their medical information. Such an algorithm could be important and useful from both an investigative and decommissioning perspective. If an investigator is able to determine who owns a particular smartphone containing medical information, it could help provide investigators with more information on the individual, whose identity might be unknown.

Acknowledgements G. Grispos was financially supported by the Nebraska Research Initiative (NRI), while the work of K.-K.R. Choo was supported by the National Security Agency (NSA) (Award H98230-20-1-0392). The statements, opinions, and content included in this publication do not necessarily reflect the position or the policy of the NRI or the NSA, and no official endorsement should be inferred.

Declarations

Conflicts of Interest There is no conflict of interest to declare, with regard to the above research.

References

1. AliveCor (2021) Kardiamobile. Available online: https://store.kardia.com/products/kardiamobile
2. Alyahya T, Kausar F (2017) Snapchat analysis to discover digital forensic artifacts on android smartphone. Proc Comp Sci 109:1035–1040
3. American Medical Association (2020) Physicians' motivations and requirements for adopting digital health adoption and attitudinal shifts from 2016 to 2019. Available Online: https://www.ama-assn.org/system/files/2020-02/ama-digital-health-study. pdf
4. Australian Government (2021) Medical device cyber security guidance for industry. Available Online: https://www.tga.gov.au/node/874778
5. Baumgart DC (2020) Digital advantage in the covid-19 response: perspective from Canada's largest integrated digitalized healthcare system. NPJ Digit Med 3(1):1–4
6. Chernyshev M, Zeadally S, Baig Z (2019) Healthcare data breaches: Implications for digital forensic readiness. J Med Syst 43(1):1–12
7. Cusack B, Kyaw AK (2012) Forensic readiness for wireless medical devices. In: 10th Australian digital forensics conference. p 21
8. Dargahi T, Dehghantanha A, Conti M (2017) Forensics analysis of android mobile voip apps. In: Contemporary digital forensic investigations of cloud and mobile applications. Elsevier, pp 7–20
9. Ellouze N, Rekhis S, Boudriga N (2016) Forensic investigation of digital crimes in healthcare applications. In: Data mining trends and applications in criminal science and investigations. IGI Global, pp 169–210
10. Ellouze N, Rekhis S, Boudriga N, Allouche M (2017) Cardiac implantable medical devices forensics: Postmortem analysis of lethal attacks scenarios. Digit Investig 21:11–30
11. European Union Agency for Network and Information Security (2017) Privacy and data protection in mobile applications: a study on the app development ecosystem and the technical implementation of GDPR. Available from https://data.europa.eu/doi/10.2824/114584. Accessed 10 Oct 2021
12. Flynn T, Grispos G, Glisson W, Mahoney W (2020) Knock! knock! who is there? investigating data leakage from a medical internet of things hijacking attack. In: 53rd Hawaii International Conference on System Sciences. Maui, Hi, USA, pp 1–10
13. Fowler J (2021) Report: Fitness tracker data breach exposed 61 million records and user data online. Available online: https://www.websiteplanet.com/blog/gethealth-leak-report/
14. Freiling F, Schwittay B (2007) A common process model for incident response and digital forensics. Proceedings of the 3rd International Conference on IT Incident Management and IT Forensics (IMF 2007), Stuttgart, Germany
15. Grispos G, Bastola K (2020) Cyber autopsies: The integration of digital forensics into medical contexts. In: 33rd international symposium on computer based medical systems (CBMS 2020). IEEE, pp. 1–4
16. Grispos G, Flynn T, Glisson W, Choo KKR (2021) Investigating protected health information leakage from android medical applications. In: 5th EAI international conference on future access enablers of ubiquitous and intelligent infrastructures (FABULOUS 2021)
17. Grispos G, Glisson W, Cooper P (2019) A bleeding digital heart: identifying residual data generation from smartphone applications interacting with medical devices. Proceedings of the 52nd Hawaii international conference on system sciences (HICSS-52), Maui, HI, USA
18. Grispos G, Glisson WB, Choo KKR (2017) Medical cyber-physical systems development: A forensics-driven approach. In: Proceedings of the Second IEEE/ACM international conference on connected health: Applications, systems and engineering technologies. IEEE, pp 108–114
19. Grispos G, Glisson WB, 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. IEEE, pp. 4910–4919
20. Grispos G, Glisson WB, Storer T (2015) Recovering residual forensic data from smartphone interactions with cloud storage providers. In: The Cloud Security Ecosystem – Technical, Legal, Business and Management Issues, chap.16. Syngress, pp 347–382
21. Grispos G, Tursi F, Choo R, Mahoney W, Glisson WB (2021) A digital forensics investigation of a smart scale iot ecosystem. Proceedings of the 20th IEEE international conference on trust, security and privacy in computing and communications (IEEE TrustCom), Online, China.

22. Hoog A (2011) Android forensics: investigation, analysis and mobile security for Google Android. 1st Ed. Syngress, Waltham, MA, USA
23. Hoog A, Strzempka K (2011) iPhone and iOS forensics: investigation, analysis and mobile security for Apple iPhone, iPad and iOS devices. 1st Ed. Syngress, Waltham, MA, USA
24. Jahankhani H, Ibarra J (2019) Digital forensic investigation for the Internet of medical things (IoMT). J Foren Legal Invest Sci 5(2):029
25. Lacour P, Buschmann C, Storm C, Nee J, Parwani AS, Huemer M, Attanasio P, Boldt LH, Rauch G, Kucher A et al (2018) Cardiac implantable electronic device interrogation at forensic autopsy: an underestimated resource? Circulation 137(25):2730–2740
26. Liu J, Sasaki R, Uehara T (2020) Towards a holistic approach to medical iot forensics. In: 2020 IEEE 20th international conference on software quality, reliability and security companion (QRS-C). IEEE, pp 686–687
27. Mahalik H, Tamma R, Bommisetty S (2016) Practical mobile forensics. 2nd Ed. Packt Publishing Ltd, Birmingham, United Kingdom
28. Maras MH, Wandt AS (2020) State of ohio v. ross compton: Internet-enabled medical device data introduced as evidence of arson and insurance fraud. Int J Evid Proof 24(3):321–328
29. Maus S, Höfken H, Schuba M (2011) Forensic analysis of geodata in android smartphones. In: International conference on cybercrime, security and digital forensics. http://www.schuba.fhaachen.de/papers/11cyberforensics.pdf
30. The MITRE Corporation (2018) Medical device cybersecurity: regional incident preparedness and response playbook. Available online: https://www.mitre.org/sites/default/files/2021-11/prs-18-1550-Medical-Device-Cybersecurity-Playbook.pdf. Accessed 10 Oct 2021
31. Mohay G (2005) Technical challenges and directions for digital forensics. In: First international workshop on systematic approaches to digital forensic engineering (SADFE'05). IEEE, pp 155–161
32. Norouzizadeh Dezfouli F, Dehghantanha A, Eterovic-Soric B, Choo KKR (2016) Investigating social networking applications on smartphones detecting facebook, twitter, linkedin and google+ artefacts on android and IoS platforms. Aust J Forensic Sci 48(4):469–488
33. Oates BJ (2005) Researching information systems and computing. 1st Ed. SAGE Publications, London, United Kingdom
34. Quick D, Choo KKR (2013) Dropbox analysis: Data remnants on user machines. Digit Investig 10(1):3–18
35. Quick D, Martini B, Choo R (2013) Cloud storage forensics. 1st Ed. Syngress, Waltham, MA, USA
36. Singh A, Wilkinson S, Braganza S (2014) Smartphones and pediatric apps to mobilize the medical home. J Pediatr 165(3):606–610
37. StatCounter (2021) Mobile Operating System Market Share Worldwide Sept 2020 - Sept 2021. Available online: https://gs.statcounter.com/os-market-share/mobile/worldwide
38. Tangari G, Ikram M, Ijaz K, Kaafar MA, Berkovsky S (2021) Mobile health and privacy: cross sectional study. BMJ 373
39. United State Food and Drug Administration (2016) Postmarket management of cybersecurity in medical devices. Available online: https://www.fda.gov/regulatoryinformation/search-fda-guidance-documents/postmarket-management-cybersecurity-medicaldevices. Accessed 10 Oct 2021
40. United State Food and Drug Administration (2020) Premarket notification 510(k). Available online: https://www.fda.gov/medical-devices/premarket-submissions/premarket-not ification-510k
41. United States Food and Drug Administration (2019) Cybersecurity. Available from: https://www.fda.gov/medical-devices/digital-health/cybersecurity
42. United States Food and Drug Administration (2019) Policy for device software functions and mobile medical applications. Available online: https://www.fda.gov/media/80958/download. Accessed 10 Oct 2021
43. The Health Insurance Portability and Accountability Act of 1996, Pub.L. 104–191 (1996) Available online: https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf. Accessed 10 Oct 2021
44. United States Government Accountability Office (2012) FDA should expand its consideration of information security for certain types of devices. Available online: https://www.gao.gov/products/gao-12-816. Accessed 10 Oct 2021
45. Verizon (2019) 2019 Mobile security index. Available online https://www.verizon.com/business/resources/reports/mobile-security-index/2019/. Accessed 10 Oct 2021