International Journal of E-Health and Medical Communications
Volume 12 • Issue 3 • May-June 2021

Regulations and Standards Aware Framework for Recording of mHealth App Vulnerabilities

Zornitza Prodanoff, University of North Florida, USA
Cynthia White-Williams, University of North Florida, USA
https://orcid.org/0000-0002-8344-7427
Hongmei Chi, Florida A&M University, USA

ABSTRACT

The authors describe a standards-based security framework for the purposes of recording security and privacy vulnerabilities discovered in mHealth apps. The proposed framework is compliant with the international standard for software architecture descriptions, ISO/IEC/IEEE 42010, relevant state-agency regulations, and US federal healthcare mandates, as well as computing standards for data interchange formats. Future real-life implementations are envisioned to consists of three key components: (1) design and implementation of a repository that links vulnerabilities to concepts from the taxonomy used by legislative and standardization bodies; (2) population of the repository with security vulnerability descriptions that follow a standard format, such as JavaScript Object Notation (JSON); and (3) implementation of a searchable user interface (e.g., Google's Firebase UI), which allows for aggregation statistics, data analytics, as well as public access to the repository. The proposed framework design promotes timely updates of regulations, standardization drafts, and app development platforms.

KEYWORDS

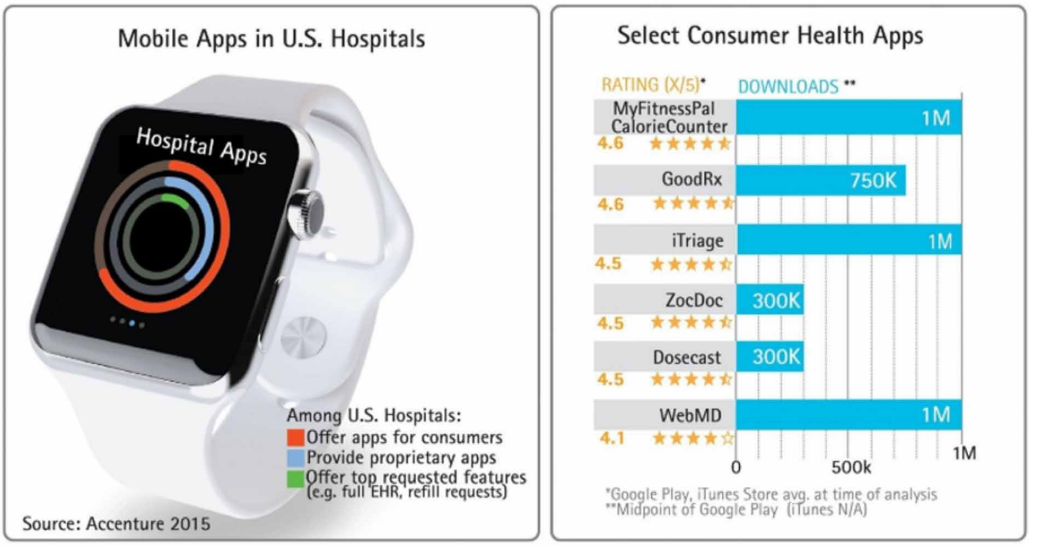
BLE, EHR, IoT, mHealth, Privacy, Regulation, RFID, Security, Standard, Vulnerability Recording

1. INTRODUCTION

Mobile computing devices are the primary tool for disseminating and using commercial, health, medical, and military applications (Avancha, et al. 2012; West & Bleiberg, 2014). The International Telecommunication Union reports that in 2013 95% of people lived in an area that is covered by cellular networks, while mobile broadband networks (3G, 4G or above) were already accessible to 84% of the global population (ITU ICT Facts and Figures, 2013). The reported popularity of smartphones has been the main driver for increase in the development and adoption of mHealth apps (Wallis, Blessing, Dalwai, & Shin, 2017). The healthcare industry has experienced a significant increase in the utilization of mHealth applications. In 2017, there were about 325,000 mHealth apps available for download (Global mHealth, 2019). Another 2017 study reported that there have been 259,000 mHealth apps available for consumer download through the major app stores (Lee & Kim, 2017). It is estimated that by 2025, mHealth apps will generate approximately $111.1 billion revenue (Global mHealth, 2019). At the same time, chronic disease has been reported as the leading cause of death

DOI: 10.4018/IJEHMC.20210501.oa1

Figure 1. Availability of mHealth Apps: Providers vs. 3-rd Party Developers (Pennic, 2016)

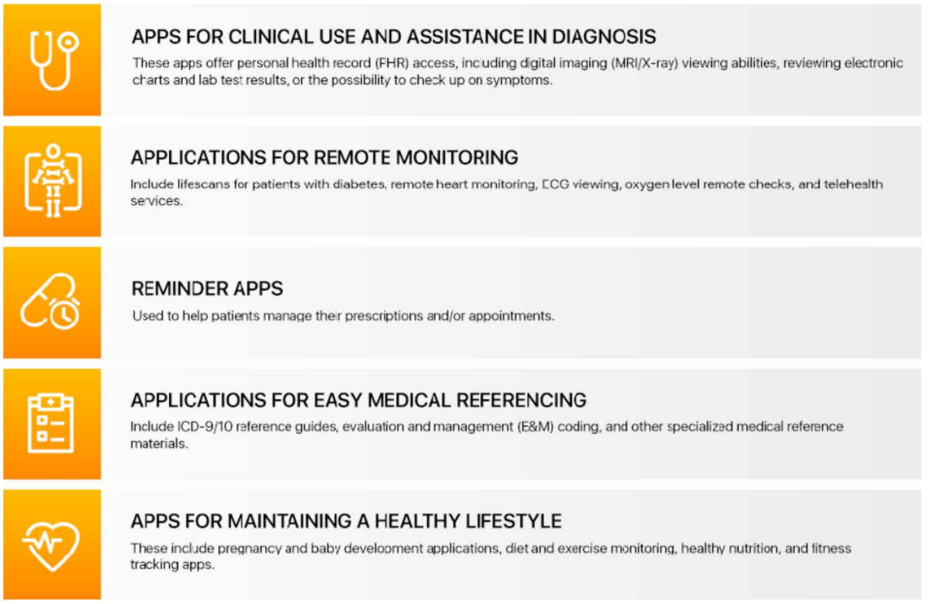


worldwide, while chronic disease management apps are projected at $15 billion, which is over 70 percent of the mHealth apps revenue (Mabo, Swar, & Aghili, 2018). For those reasons, mHealth apps have been instituted in general to mitigate the mortality rate associated with chronic diseases through overall disease management or prevention approaches. As depicted in Figure 1, mHealth apps are widely offered by both healthcare providers and third party developers alike. These devices range from communication capabilities, health information systems, informational resources, and clinical software applications (Ventola, 2014).

1.1. Growing Popularity of mHealth Systems Using IoT Technologies

The healthcare industry is one of the most attractive applications of Internet of Things (IoT). Due to the increase complexity of healthcare services and the integration of technology, IoT is touted for its ability to "intelligentize" medical service systems (Yin, et al., 2016). The market for health IoT is expected to reach $117 billion by 2020 and include some 26 billion devices (Williams & McCauley, 2016). By mobilizing computing medical sensors and various communication technologies for healthcare services, the network of healthcare resources are extended across hospital, clinics, communities, and homes (Alam, et al., 2018; Slam, et al., 2015). An IoT based healthcare system connects available resources across a network to perform diagnosing, monitoring, and surgeries over the internet (Yin, et al., 2016). The progress in healthcare monitoring and control, interoperability and security, and medication management have demonstrated the potential to effectively use technology while providing patient-centered care (Yin, et al., 2016). The potential for pervasive communications amongst things and people allow for interactions between users, Radio Frequency Identification (RFID) tags, sensors, and PDAs in order to support real-time data updates and decision-making activities (Yin, et al., 2016). In an aging population for example, IoT services may create ambient assisted living environments, in which an integration of automation, security, control, and communication is provided in the patient's preferred place of living. Underlying this technology is 6LoWPAN, RFID and Near-Field Communication (NFC). This architecture can be extended to include medical knowledge for "medically-complex" individuals (Slam, et al., 2015). The resultant infrastructure is communication among stakeholder such as the elderly adults, caregivers, physicians, and family (Slam et al., 2015). By using an open, secure, and flexible platform based on the IoT and computing,

Figure 2. Types of mHealth Apps (Garth, 2018)



issues such as security, interoperability, data storage, and flexibility are mitigated with an IoT-based health gateway as a reference implementation. A noticeable recent trend has been a sustained vendor interest in manufacturing mobile phones compatible with multiple IoT technologies, such as NFC, compatible with high frequency (HF) RFID, and Bluetooth Smart. Merging of the Web, RFID, NFC, and Bluetooth technologies is already done by means of widely available NFC-enabled and Bluetooth-enabled smartphones. Such devices could be used as HF RFID readers to, for example, to track medical supplies or to interact with Bluetooth smart beacons with the goal of proving customized functionality that targets individual patients. Drop in prices of RFID tags allowed for large scale RFID networks deployment in the healthcare industry for the purposes of inventory control (Najera, 2011), (Ranasinghe, et al., 2010), newborn and patient tracking and identification (Hung, 2011; Leu, 2010) treatment/supplies tracking (Katz & Rice, 2009), surgical process management (Yao, 2012). Saint Joseph's Hospital, a 410-bed facility located in Atlanta, Ga., uses HF RFID technology and a Web-based information system for inventory control of high-cost medical devices valued at $2 million in its cardiac catheterization and electrophysiology units ("RFID in Health Care Presentations", 2018). Chang-Gung Memorial Hospital (CGMH) in Taipei, Taiwan has implemented since 2007 HF RFID wristbands for patients in its surgical and neonatal units (Bacheldor, et al., 2014). A Czech hospital uses HF RFID to track Chemotherapy Drugs (Wessel, 2018).

Figure 2 presents an overview of the common types of mHealth Apps. It is important to emphasize that multiple type of connectivity technologies are sometimes used to implement mHealth app in the five categories listed in Figure 2. This opens up such apps to security and privacy vulnerabilities through multiple networking interfaces using IoT communications technologies. (Note that ICD-10 is the 10th revision (that updates ICD-9) from the International Classification of Diseases (ICD) that was adopted in multiple countries on October 1, 2015).

This article is organized as follows. Section II contains an overview of previous work and discusses the need for standards-based recording of security vulnerabilities for mHealth apps and alignment of governmental regulations with such recording. Patient and user security, privacy, and data integrity for mHealth apps are of critical importance. Yet, devices are widely used while rarely adequately secured. Governmental bodies have recognized the need to address this problem by producing and

continuously improving the relevance of security and privacy legislations, however, computer security professionals and hackers, who are the primary initiators of vulnerability recording, rarely address the connection between specific device vulnerabilities and regulatory implications. The lack of a streamlined process of linking security and privacy vulnerabilities to specific regulations and industry-wide standards is an unresolved pressing need that negatively affects the safe operation of mHealth apps. That need is illustrated in more detail in Section III through the results of a case study we conducted examining mHealth relevant regulations for governmental agencies in the state of Florida. Our proposed framework that addresses the challenges presented in Sections II and III is described in Section IV. It consists of a model for a vulnerability recording process that is streamlined through the use of a structured file format (e.g. JSON) and a searchable user interface (UI) to a database (e.g. Google's Firebase UI) with added data analytics and aggregation statistics service (e.g. "Elastisearch", 2018). Summary and future work ideas are described in Section V.

2. RELATED WORK

Although the scientific community has been documenting the security and privacy vulnerabilities of mHealth apps and devices, the problem of aligning governmental regulations with security and privacy vulnerability recording as well as with provisions in standardization drafts has not been extensively studied yet.

2.1. Documenting Security and Privacy Vulnerabilities of mHealth Apps

The scientific community has historically documented security and privacy concerns for mHealth applications. Healthcare is unique in that the "quality, provenance, traceability, integrity and authenticity of data is critically important" (Williams & McCauley, 2016). This reality has significant implications on patient's quality of life, privacy, and security that should be comprehensively addressed in the design and development of applications. Yet, devices running mHealth apps are usually inadequately secured. O'Loughlin and colleagues (2019) systematic review of 116 mHealth apps suggest that only 4 percent (5/116) had acceptable privacy policies, while less than half had any privacy policy. Since many mHealth applications collect personal information, the privacy concerns are complex when data are being shared among devices and between cloud services and devices. This is due in part to the lack of encryption, network mis-configuration and the lack of security education (Williams & McCauley, 2017). Despite the heightened security awareness and recent attacks such as the May 2017 WannaCry attack and the October 2016 Distributed Denial of Services, the current systems continues to have significant vulnerability to cyberattacks (Kirtley & Memmel, 2018).

The portability and powerful computing capabilities of smartphones allow people to connect anytime and anywhere. Their popularity, however, makes them ideal targets for security breaches. Another reason for the often compromised security of mobile devices is due to their limited resource capabilities that result in an inherent trade-off between device performance and complete (as opposed to partial) feature implementation of security protocols. The rise in the number and sophistication of threats and the broadening vulnerabilities of mobile apps and systems worldwide has been well documented already (Paul, et al., 2013), (Pournaghshband, et al., 2013). In addition to being prone to security vulnerabilities, mHealth apps are vulnerable to compromises on user privacy. Given the vast popularity of mHealth apps, it is a quite disturbing trend that a large percentage of mobile health applications have been found to actively collect users' sensitive information and to send it to vendors or third-party domains over HTTP (Papageorgiou, et al., 2018). Moreover, such transmissions are typically done "in the clear", using plaintext without encryption.

2.2. Security and Privacy of mHealth Apps Using IoT Communication Technologies

Most common security attacks on RFID include jamming, eavesdropping, replay attack, tag deactivation, tag detaching, spoofing, man-in-the-middle attack, and cloning. Some of the above

threats are physical/mechanical in nature and no security protocol can protect against them, e.g. tag deactivation (via physical destruction, not kill command), tag detaching. In addition, passive tags are small in size and low in price, which results in lack of implementation of sophisticated security protocol rules and algorithms. There are some existing standards that provide security measures for RFID networks, e.g. ISO/IEC 29167 (ISO/IEC 29167-1, 2018), but they are vulnerable to man-in-the middle and other attacks (Song, et al., 2012). HF tags are inherently secure because of the typical reading range of a few inches or less, but are still susceptible to man-in-the middle attacks (Song, et al., 2012). According to Monika Adarsh, a tech blogger for Beaconstac.com, healthcare related orders of Bluetooth beacon, comprised 20% of the market share in 2015 and exhibit an ever-increasing trend as of September of 2018 (Adarsh, 2018). When a patient reaches the premises of a medical facility, Bluetooth Smart beacons could be strategically positioned at the entrance and automatically open a map to the patient's appointment venue or display breakfast coupons information at the cafeteria through push notifications (Adarsh, 2018). In addition, the widely popular wearable Bluetooth Smart devices such as Fitbit and other fitness and health tracker devices are also designed to interface with mobile phones. The Bluetooth protocols provide adequate authentication for device pairing purposes, however, connection confidentiality is implemented optionally. Although the Bluetooth standards provide for confidentiality of the exchanged data, once the devices are authenticated through pairing, the choice of encrypted vs. unprotected connection establishment is left up to the mobile app developer.

2.3. The Disconnect Between Regulations, Standards, and Vulnerability Recording

The disconnect between regulations, standards, and vulnerability recording appears to be the results of several major challenges. Although it has been shown that implementing healthcare systems by following related regulations and standards has positive outcomes, not all vendors follow standardization drafts that ensure interoperability within eHealth systems. The benefit of using healthcare related standards for chronic disease management have been studied before. Sloane and Gehlot have demonstrated how relatively low cost devices, software, systems, and encryption services can be combined to provide chronic disease management and population health surveillance using existing standards (Sloane and Gehlot, 2016). Nevertheless, many vendors do not follow standardization in terms of technical issues such as "communications layers and protocol stacks, including physical (PHY) and media access control (MAC) layers, device interfaces, data aggregation interfaces, and gateway interfaces" (Islam, et al., 2015). This leads to interoperability issues. The potential impact of newly discovered vulnerabilities on such systems becomes unpredictable and difficult to document. Another disconnect exists between mitigation approaches against security threats for IoT devices as proposed by the scientific community versus published and known vulnerability recordings. For example, Strielkina and colleagues developed an interesting technique for preventing attacks on vulnerabilities of the healthcare IoT infrastructure using Markov models (Strielkina, et al., 2018). However, their study does not mention any specific previously published vulnerability recordings, relevant governmental regulations, or standards. A third challenge is the limited availability of privacy-related regulations as discussed by Iwaya (Iwaya et.al., 2018) in the context of the EU Directive 95/461EC which is regarded as one of the few globally available comprehensive regulatory documents protecting individual's privacy. EU Directive 95/461EC includes provisions for protecting the health data of individuals using one of the most recognized taxonomies of privacy threats (Oetzel and Spiekermann, 2014). According to the Third Global Survey on eHealth conducted by the World Health Organization only 54% of global responders indicated that the policy or legislation in their respective countries "protects the privacy of individuals' health-related data held in electronic format" (WHO, 2016).

Table 1. Detection and response functions (Section 74-2 of FAC, 2018)

Detect	Anomalies & Events Security Continuous Monitoring Detection Processes
Respond	Response Planning Communications Analysis Mitigation Improvements

3. CASE STUDY: MHEALTH SYSTEMS SECURITY AND PRIVACY REGULATIONS IN FLORIDA

Next, we present an illustrative case study of current governmental regulations related to state agency mHealth systems security and privacy in the State of Florida and their compatibility with vulnerability recording practices and standards.

A noticeable trend in advances of mobile computing and IoT technologies as well as Electronic Health Records (EHR) incentive programs, enabled a growing number of Florida state agencies' employees to access healthcare data and resources through mobile devices. For example, employees of the Agency for Healthcare Administration (AHCA) or eligible hospital and Medicaid providers may soon allow restricted access to Electronic Health Records via mobile devices as part of the Medicare and Medicaid Promoting Interoperability (PI) Program. The example is not limited to that agency. Employees of other Florida state agencies may soon be able to access EHR records via mobile devices, as well, including the Agency for Persons with Disabilities (APD), Department of Children and Families, Bureau Of Exceptional Education And Student Services, Florida Department of Elder Affairs, Department of Health, Children's Medical Services, Florida Department of Veterans Affairs, Division of Blind Services, Division of Vocational Rehabilitation, Florida Alliance for Assistive Services and Technologies (FAAST).

IoT devices are not typically designed with security as the primary goal. Those devices also operate as unsecured (or inadequately secured) communication endpoints and with known vulnerabilities and little ability to receive updates (as downtime for security maintenance does not typically occur). In addition, a most vulnerable user group is patients using pacemakers, defibrillators and insulin pumps, etc. Security breaches have significant implications on the operation of such healthcare devices and pose an obvious risk to user safety. Employees of state agencies at a great risk of involuntary

Table 2. Required continuous monitoring activities (Section 74-2 of FAC, 2018)

(a)	Monitoring the network to detect potential cybersecurity events (DE.CM-1).
(b)	Monitoring for unauthorized IT resource connections to the internal agency network.
(c)	Monitoring the physical environment to detect potential cybersecurity events (DE.CM-2).
(d)	Monitoring user activity to detect potential cybersecurity events (DE.CM-3).
(e)	Monitoring for malicious code (DE.CM-4).
(f)	Monitoring for unauthorized mobile code (DE.CM-5).
(g)	Monitoring external service provider activity to detect cybersecurity events (DE.CM-6).
(h)	Monitoring for unauthorized personnel, connections, devices, and software (DE.CM-7).
(i)	Performing vulnerability scans (DE.CM-8). These shall be a part of the SDLC.

unauthorized disclosure of EHR data as well as their personal data, as their devices are prone to all vulnerabilities that could directly result in unauthorized disclosure or various other security issues such as compromises in data integrity or data access and service availability. Legislative efforts to address this issue resulted in the development of The Florida Cybersecurity Standards (FCS), a set of risk assessment requirements for Florida state agencies that are outlined in section 282.318 of the Florida Statutes and in the Florida Cybersecurity Standards of section 74-2 of the Florida Administrative Code (Section 74-2 of FAC, 2018). The detection and response functions that are required to be implemented by the computer and communications systems of individual agencies are outlined in Table 1. A list of continuous monitoring activities that agencies in the State of Florida are required to perform by Chapter 74-2 of the Florida Administrative Code is shown in Table 2. Those are described as part of the "detect function" of the FCS. To meet those requirements each agency has to have processes in place to detect anomalies and security breaches, to continuously monitor its systems for such events, and finally, to detect security events as they occur. Once detected, anomalies and security events are to be acted upon as outlined in Table 1: via response and planning processes, communications, analysis, mitigation, and improvements.

3.1. The Missing Link: Standardization of Reporting vs. Low-Level Technical Terminology

Fortunately, computer systems have been traditionally designed with elaborate event logging capabilities that provide a necessary tool set for network administrators and IT security specialists in charge of the systems considered above. Figure 3 presents a visualization of a typical event log record from a mobile device that contains a list of operating systems processes as they are occurring. The depicted example is for an app that is designed to transfer large files on an Android device by evoking both the built-in Bluetooth and the NFC antennae. It is interesting to observe the multitasking nature of Android by noting that log entries from system-level processes with UIDs identifiers in the range between 1000 and 2999 are interleaved with entries generated by user-level app processes (UIDs greater than 9,999). Figure 3 depicts the complexity of app execution as an interaction between a mix of background OS process and user-level processes on a powered up mobile device. The challenge is to take advantage of such low-level OS details in order to describe mHealth app vulnerabilities in terms consistent with both government standards and OS constructs.

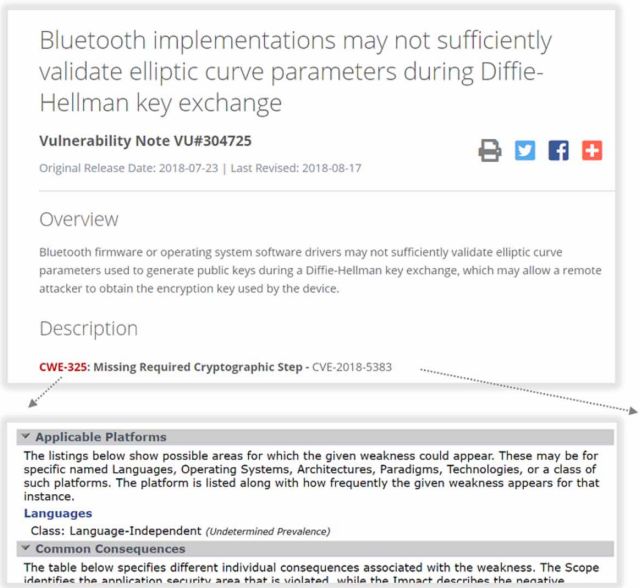
A closer examination of Vulnerability Note VU#304725 that was released on 7/23/2018 and last revised on 8/17/2018, shown in Figure 4, reveals that OS details are not provided in the Applicable Platforms field, although OS software drivers are mentioned in the vulnerability note's overview. We believe that further details about specific OS platforms and respective processes that are affected would not only help the developer's community to address the issue, but would also create a framework to link future related vulnerability notes to this instance. Such framework would provide the user interface to record technical constructs such as, but not limited to: affected OS-level processes, affected OS implementation classes (e.g. any of specific methods of the AdapterService class objects used by Android, or any specific methods of the CBCentralManager class in iOS), etc.

To further illustrate the need for more technically aware recording and regulatory draft writing, we performed linguistics frequency analysis using the Text Analyzer utility (Adamovic, 2019). We analyzed several documents: State of Florida regulations, vulnerability note, OS documentation, and industry best practices specification. The results are presented in Table 3. The reader should note that the LogCat and the Android App Security Best Practices documents, both published by the Android developers' community, are technical drafts that contain specific hardware and operating systems relevant details. A quick examination of the list of commonly used words in each comparison pair shows that very little relevant technical terminology such as OS, software, or hardware-level process execution related concepts are used in governmental regulations and even in vulnerability recording notes. This apparent disconnect between more general regulatory expectations and the technicalities of their implementation creates unnecessary ambiguity for network administrators and security

Figure 3. LogCat Snippet from App Execution on a Samsung Galaxy Note 8 (Android 7.0 Nougat)

```
10-27 11:06:43.576 D/WifiConnectivityMonitor(1446):  [|210]
10-27 11:06:43.755 D/bauth_FPBAuthService(1076): pcf : 0x1012
10-27 11:06:43.905 I/WifiTrafficPoller(1446): mCpuCoreBooster Lock
10-27 11:08:16.537 D/audio_hw_primary(624): enable_audio_route: apply mixer and update path: deep-buffer-playback speaker
10-27 11:08:16.604 I/WifiTrafficPoller(1446): mCpuCoreBooster Lock
10-27 11:08:16.649 D/BeamManager(2583): isBeamInProgress() is false
10-27 11:08:16.649 I/NfcP2pLinkManager(2583): trySBeamRecord
10-27 11:08:16.649 I/NfcP2pLinkManager(2583): trySBeamRecord : there's no sbeam record.
10-27 11:08:16.651 D/ViewRootImpl@3e6a1fb[MainActivity](27120): MSG_WINDOW_FOCUS_CHANGED 0
10-27 11:08:16.680 I/SurfaceFlinger(668): Display 0 HWC layers:
10-27 11:08:16.680 I/SurfaceFlinger(668):      Device | 0x797a1c4200 |com.example.android.beamlargefiles
10-27 11:08:16.680 I/SurfaceFlinger(668):      Device | 0x7979e3cc80 |#0
10-27 11:08:16.680 I/SurfaceFlinger(668):      Device | 0x797a1c4c00 |StatusBar#0
10-27 11:08:54.766 D/DnsProxyListener(976): DNSDBG::dns addrinfo af 2
10-27 11:08:54.790 I/WifiTrafficPoller(1446): mCpuCoreBooster Lock
10-27 11:09:13.521 D/BluetoothAdapterService(7005): updateEvent call by com.android.nfc, isEnable : false
10-27 11:09:13.557 D/AdapterProvider(7005): update
10-27 11:09:13.559 E/BluetoothAdapterService(7005): updateEvent - update success 1
10-27 11:09:13.566 D/BeamManager(2583): MSG_SEND_LOG / send Big Data Log
10-27 11:09:13.566 D/BeamManager(2583): msg.what is 288 so mBeamInProgress is false
10-27 11:09:13.566 E/NfcLogManager(2583): insertLog::feature=P2PF
10-27 11:09:13.567 D/BluetoothAdapterService(7005): disable() called...
```

Figure 4. Vulnerability Note VU#304725 (Vulnerability Note VU#304725, 2018)



professionals responsible for the implementation of security and privacy practices that comply with imposed expectations. More importantly, this disconnect in common terminology does not support a streamlined process of linking known vulnerabilities with potential loss of compliance with specific government regulations and industry practices.

4. PROPOSED FRAMEWORK FOR RECORDING VULNERABILITIES OF MHEALTH APPS

MHealth apps are different from other mobile apps, as they are subject to much global, governmental, and industry standardization. Oversight and regulations are needed mainly for patient well-being and (user) security and privacy reasons. Standardization is driven by multiple factors, including efficient

sharing of EHR data between providers, patients, and third parties, as well as platform compatibility between mHealth apps and cloud services. Figure 5 depicts the limitations and constraints that need to be addressed through the recording process, ensuring that vulnerability recordings not only describe the nature of security and privacy vulnerability in question, but also its particular relevance to specific governmental regulations, industry standards, as well as proprietary device implementations.

A high-level overview of our proposed framework for recording of vulnerabilities of mHealth apps is shown in Figure 6. We propose that the vulnerability recording process includes three main layers for incorporating important regulations, standards, and other limitation (constraints) into each recordings: Application Layer, Network & Cloud Services layer, and Device & Vendor-specific layer. Ensuring the security and privacy of mHealth app users presents a unique recording challenge because of the diversity and complexity of those apps. Hence, in Figure 6, we present our framework through the example of one specific mHealth app vendor, Fitbit. It is interesting to note that we provide examples of only about a dozen specific regulations, standards, and device limitation; however, there are other common practices and standards that are not shown for brevity purposes. We propose to design the vulnerability recording process to specifically address any relevant provisions stemming from regulation, standardization, as well as implementation limitations. Existing public vulnerability databases are generally designed to assign unique vulnerability identifiers in standardized format and offer plausible workarounds and sometimes even threat mitigation. We extend this model in order to incorporate any constraints imposed by regulations, standardization documents, and device limitations (e.g. assumed syntax used by iOS, effective NFC antenna range of the NXP NTAG213F chip, etc.). Our newly proposed approach would be novel in its ability to facilitate assessments such as vulnerability risk scores and impact ratings while ensuring such quantification is meaningful in the context of governmental regulations and standardization.

Databases for security and privacy vulnerabilities of any computing devices and systems have already been implemented and made openly available through searchable Web interfaces. Hence, the recording process would need to be compliant with existing recording standards used by the relevant repositories. Examples include the Common Vulnerabilities and Exposures (CVE) specification (CVE, 2018) and the Common Vulnerability Scoring System (CVSS) v3.0 (First.org, 2018), a specification draft issued by The Forum of Incident Response and Security Teams (FIRST), a global association of the Computer Emergency Response Team (CERT) (CERT, 2018). An example of such vulnerability recording in standard format is Vulnerability Note VU#176301 (Vulnerability Note VU#176301, 2018) as recorded by the Carnegie Mellon University's CERT Coordination Center of the CMU Software Engineering Institute. Currently, security and privacy vulnerabilities stored in such databases are typically described via high-level OS constructs and other technical terms, but rarely refer to applicable regulations and standards. As shown in Figure 6, Fitbit Flex uses the Texas Instruments CC2540 microcontroller. Vulnerability Note VU#317277 (CVE CVE-2018-7080 - also known as BLEEDINGBIT) describes a known vulnerability of the CC2540 chip implementation. Yet, the recording does not mention how that vulnerability affects cryptographic control of sensitive data or management and protection of encryption keys – pivotal points of the provisions in the ISO 27799 standard covering protection of personal health data. To streamline the recording process and ensure that it is compatible with existing publicly available vulnerability databases, we further propose that recordings could be generated following the JavaScript Object Notation (JSON) format (ECMA-404, 2017). JSON format recording would add a design layer that would facilitates the compatibility of global and governmental regulations, as well as industry standards and vendor support. For example, if any mHealth related State of Florida .gov Web site vulnerabilities are identified, it would constitute a good practice to submit a report to CERT via their "How to Report a Vulnerability" user interface (CERT/CC, 2018) that includes a vulnerability description in JSON format with specific references to affected sections of state and federal regulations. It would also be beneficial for public access purposes to make available any security vulnerabilities of mHealth apps that are not related to compromising access to .gov Web sites. A searchable Firebase Real Time database with added Elasticsearch service

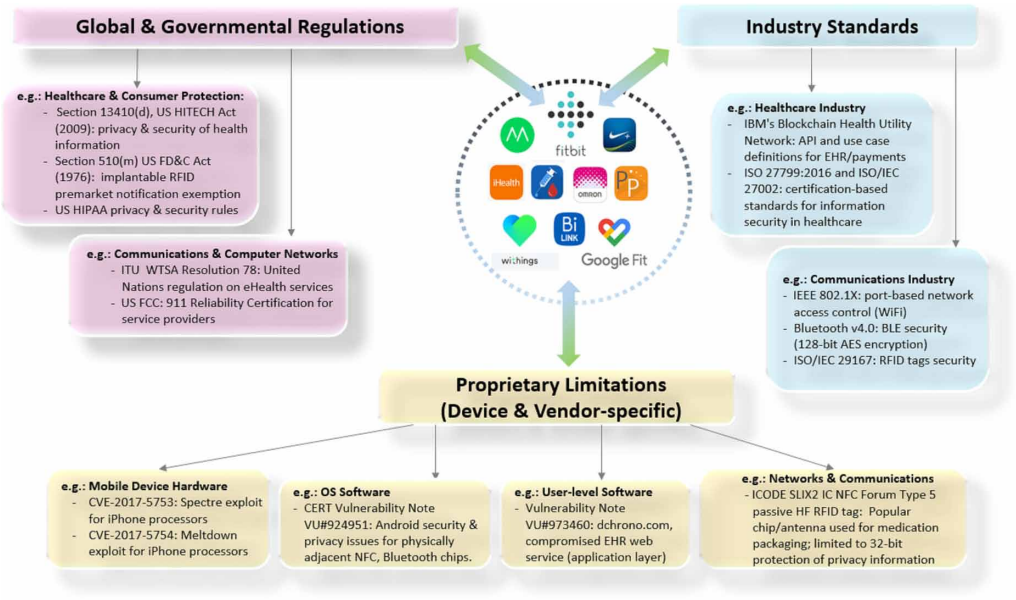
Table 3. Frequency analysis and words overlap of text documents

	LogCat (Figure 3)	**VU#304725**	**FCS Rule 60GG-2.004**	**CVSSv3.0**	**Android App Security Best Practices**
Number of characters (including spaces):	12789	4016	4285	59203	20468
Number of characters (without spaces):	9925	3273	3415	44560	15942
Number of words:	2100	592	630	8583	2803
Lexical Density:	26.619	49.1554	30.7937	17.3482	28.3625
Number of sentences:	131	33	74	720	204
Number of syllables:	3381	1132	1302	16015	5472
	Words Common to Both Compared Documents				
LogCat vs. VU#304725	*the, and, of, is, for, with, messages, can, that, system, or, from, view, as, filter, content, any, android, other, does, since, more, note, specifications, utc*				
LogCat vs. FCS Rule 60GG-2.004	*the, and, to, of, a, is, for, with, that, system, or, from, all, as, this, following, it, on, level, event, include, information, events, each, such, be, ensure, multiple, code, these, access, ensuring, connected, activity, development, methods, environment, resources, identify, will*				
CVSSv3.0 vs. FCS Rule 60GG-2.004	*and, to, the, cybersecurity, of, for, potential, that, processes, a, unauthorized, agency, network, ensure, data, information, or, code, such, impact, connections, each, be, is, it, from, malicious, access, physical, systems, this, security, multiple, users, vulnerability, environment, expected, should, understand, sources, function, include, software, requirements, incident, attack, must, collect, these, all, applicable, will, with, service, modification, as, on, improve, connected, resource, perform, them, authority, defining, part, regarding, define, development, implement, life, occur, accessing, measures, necessary, based, following, user, represented, communicating, resources, verify, level, system, assigned*				
FCS Rule 60GG-2.004 vs. Android App Security Best Practices	*the, key, to, a, of, device, and, public, by, in, information, may, all, are, for, not, an, on, date, has, be, this, messages, shared, within, can, allow, with, which, exchange, security, determine, users, secure, private, based, devices, http, updated, updates, their, during, //www, before, system, also, update, such, addition, as, https, if, is, or, from, received, unknown, that, other, impact, testing, consult, issued, first, should, google, program, html, section, content, communication, network, view, more, require, must, release, any, apply, found, between, website, note, check, added, some, android, simple*				

is a user-friendly example of such implementation that would allow for searches across multiple attributes. Multiple attribute searches would ensure that regulations and standardization constructs are linked to vulnerability descriptions and threat mitigation suggestions. Elasticsearch (Elasticsearch, 2018) is an open source RESTful search and analytics engine that is compatible with JSON. Adding such service to a recording repository could provide data analytics and aggregation statistics about specific vulnerabilities in real-time. A real-time performance evaluation under different network environments is proposed, as well.

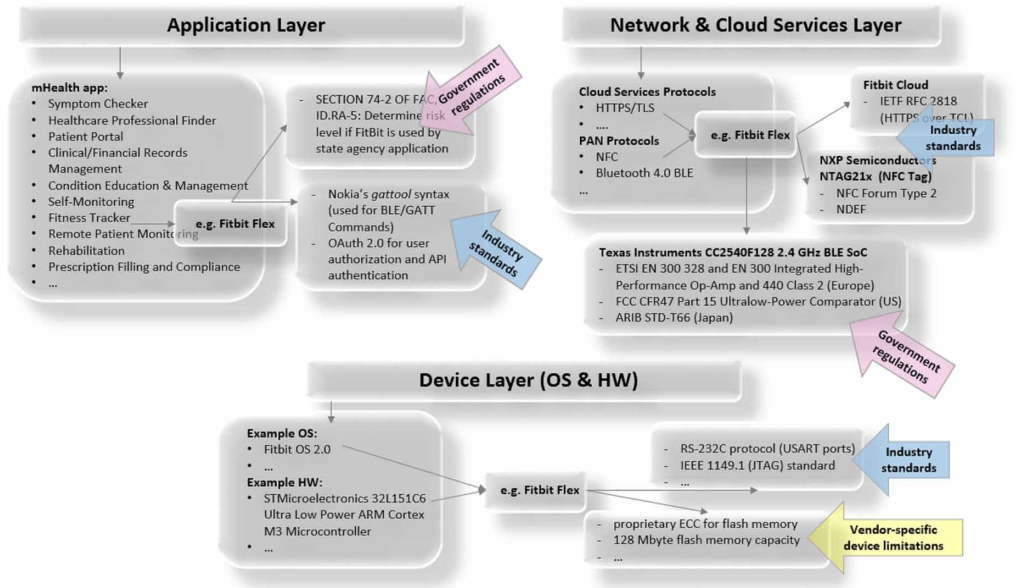
Our proposed framework design is compatible with both the currently used approaches to clinical data management via cloud services as well as emerging ones. Security features of mHealth apps and IoT devices should be developed with patient security in mind (Kirtley & Memmel, 2018). Thus, such devices are generally standardized to manage data across the traditionally used workflow of typical clinical information. It may be prudent, however, to also consider a more decentralized approach to network security. Using peer-to-peer decentralized technology such as blockchain may provide for

Figure 5. mHealth app security and privacy limitations: regulatory, industry standardization-based, and proprietary



secure access to health systems such as electronic medical devices and medical wireless body area networks (WBANs). A cryptographic approach applied to blockchain may be used to manage clinical data processes amongst devices. However the storage of large amounts of data may be inefficient for blockchain technology unless a large underlying infrastructure is built to support it. Industry interest, however, is growing fast and catching up with the opportunities offered by the blockchain technology. For example, IBM Blockchain is a public cloud service that customers can use to build

Figure 6. Regulation and standardization aware vulnerability recording framework for mHealth apps



secure blockchain networks that utilize the Linux Foundation Hyperledger Fabric v 1.0 technology. IBM has also initiated the formation of a large industry consortium (Health Utility Network) that includes health insurance companies such as Cigna, Aetna (CVS subsidiary), Anthem, Health Care Service Corporation and others. The list includes many of the companies currently reported by Forbes in the Forbes Blockchain 50 list. (Rifi, et al. 2018; Ichikawa, et al., 2017) suggested that by applying a hyperledger fabric ledger network to mHealth database it would be robust against networks faults, providing a tamper resistant system where distributed data could be used for clinical decision-making. Our framework is compatible with both the centralized and distributed approach to clinical data management.

5. SUMMARY

The problem of ensuring mHealth apps user's security and privacy is of utmost importance and requires significant alignment among legislation, industry practices, and consumers (patients or health enthusiasts). Current solutions include policy-based access to controlled data. However, control of these devices is not within the purview of single organizations or users. This is particularly concerning where devices include mHealth apps that rely on personal (patient) devices using the widely applied 'bring your own device' (BYOD) model. The problem could be better addressed through adequate coordination between global and governmental agencies as well as industry consortia. In particular, the app developer community could benefit from more streamlined process of recording and linking of mHealth app vulnerabilities to specific regulations and standards. We have presented an illustrative case study of current governmental agency regulations in the State of Florida that depicts this disconnect in more detail.

We are proposing a framework for standards-based recording and access to security vulnerability descriptions for commonly used mHealth apps that would ensure such coordination. Real-life implementation of our framework would include a repository implementations that link vulnerabilities to concepts from the taxonomy used by legislative and standardization bodies automatically, e.g. by the use of natural language processing techniques. Populating of the repositories with security vulnerability descriptions that follow a standard format, such as the JavaScript Object Notation (JSON), is a crucial step, not only to ensure fast search processing and timely access to repository data, but also compatibility between government regulations, industry practices, and standards. Allowing public access to the repository through a separate implementation of a user interface that allows for aggregation statistics as well as multi-attribute searches is an important last step in the vulnerability recording and retrieval process that ensures regulatory and standardization transparency. Such UI (e.g. Google's Firebase with added Elastisearch service) would allow patients and the general public to access vulnerability information in a more timely and efficient manner. It would also facilitate faster regulatory and standardization updates as well as threat mitigation and allow patients to more easily comprehend the implications of specific threats to their own personal privacy and security.

REFERENCES

Adamovic, M. (n.d.). *Text Analyzer Utility for Chrome OS, Version 2.0, 2006-2019*. https://www.online-utility.org/text/analyzer.jsp

Adarsh, M. (2018). *Healthcare technology: 9 ways BLE beacons are transforming healthcare in 2018*. https://blog.beaconstac.com/2018/09/healthcare-technology-9-ways-ble-beacons-are-transforming-healthcare-in-2018/

Alam, M. M., Malik, H., Khan, M. I., Pardy, T., Kuusik, A., & Le Moullec, Y. (2018). A survey on the roles of communication technologies in IoT-based personalized healthcare applications. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 36611–36631. doi:10.1109/ACCESS.2018.2853148

Aloi, G., Caliciuri, G., Fortino, G., Gravina, R., Pace, P., Russo, W., & Savaglio, C. (2017). Enabling IoT interoperability through opportunistic smartphone-based mobile gateways. *Journal of Network and Computer Applications*, *81*, 74–84. doi:10.1016/j.jnca.2016.10.013

Avancha, S., Baxi, A., & Kotz, D. (2012). Privacy in mobile technology for personal healthcare. *ACM Computing Surveys*, *45*(1), 3. doi:10.1145/2379776.2379779

Bacheldor, B. (n.d.). *Taiwan's Chang-Gung Hospital Uses HF RFID to Track Surgery*. http://www.rfidjournal.com/articles/view?2954

Bhatt, C., Dey, N., & Ashour, A. S. (Eds.). (2017). *Internet of things and big data technologies for next generation healthcare*. doi:10.1007/978-3-319-49736-5

Common Vulnerabilities and Exposures (CVE): The Standard for Information Security Vulnerability Names. (n.d.). https://cveform.mitre.org/

Common Vulnerability Scoring System v3.0: Specification Document. (n.d.). First.org Inc. https://www.first.org/cvss/specification-document

Computer Emergency Response Team (CERT). a division of the Software Engineering Institute at Carnegie Mellon University. (n.d.). https://www.sei.cmu.edu/about/divisions/cert/

Dhanvijay, M. M., & Patil, S. C. (2019). Internet of Things: A Survey of Enabling Technologies in Healthcare and its Applications. *Computer Networks*.

Elasticsearch: The Heart of the Elastic Stack. (n.d.). Elasticsearch BV. https://www.elastic.co/products/elasticsearch

Elazhary, H. (2019). Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions. *Journal of Network and Computer Applications*, *128*, 105–140.

Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., & Mankodiya, K. (2018). Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Generation Computer Systems*, *78*(Part 2), 659–676.

Garth. (2018). How to Build an Effective Medical Mobile App. *Youth Democracy*. http://www.youthdemocracy.net/build-effective-medical-mobile-app/

GDPR. (2015). *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. EU Commission.

Global mHealth Apps Market Will Reach USD 111.1 Billion By 2025: Zion Market Research. (n.d.). Retrieved from https://www.globenewswire.com/news-release/2019/01/24/1704860/0/en/Global-mHealth-Apps-Market-Will-Reach-USD-111-1-Billion-By-2025-Zion-Market-Research.html

How to Report a Vulnerability. (n.d.). Computer Emergency Response Team (CERT) Coordination Center (CERT/CC). https://vulcoord.cert.org/VulReport/

Hung, Y. (2011). *The study of adopting RFID technology in medical institute with the perspectives of cost benefit* (Ph.D. dissertation). Department of Computer Science & Information Engineering, Fu Jen Catholic University Taiwan.

Ichikawa, D., Kashiyama, M., & Ueno, T. (2017). Tamper-resistant mobile health using blockchain technology. *JMIR mHealth and uHealth*, *5*(7), e111.

Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. (2015). The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access: Practical Innovations, Open Solutions*, *3*, 678–708.

Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: A comprehensive survey. *IEEE Access: Practical Innovations, Open Solutions*, *3*, 678–708.

ISO 27799. (n.d.). *ISO 27799 — Information security management in health using ISO/IEC 27002 - guides health industry organizations on how to protect personal health information using ISO/IEC 27002". Technical Committee: ISO/TC 215 Health informatics*. Retrieved from https://www.iso.org/standard/62777.html

ISO/IEC 29167-1. (n.d.). *Information technology — Automatic Identification and Data Capture Technique.* https://www.iso.org/standard/61128.html

ITU ICT Facts and Figures. (n.d.). Retrieved 8 July, 2019, from https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf

Iwaya, L. H., Fischer-Hübner, S., Åhlfeldt, R., & Martucci, L. A. (2018). mHealth: A Privacy Threat Analysis for Public Health Surveillance Systems. *2018 IEEE 31st International Symposium on Computer-Based Medical Systems (CBMS)*, 42-47.

Kang, S., Baek, H., Jung, E., Hwang, H., & Yoo, S. (2019). Survey on the demand for adoption of Internet of Things (IoT)-based services in hospitals: Investigation of nurses' perception in a tertiary university hospital. *Applied Nursing Research*, *47*, 18–23.

Katz, J., & Rice, R. (2009). Public views of mobile medical devices and services: A US national survey of consumer sentiments towards RFID healthcare technology. *International Journal of Medical Informatics*, *78*(2), 104–114.

Kaur, B., & Dhir, V. (2017). Internet of things: Vision, Challenges and Future Scope. *International Journal of Advanced Research in Computer Science*, *8*(4), 40–43.

Kirtley, J., & Memmel, S. (2018). Too Smart for Its Own Good: Addressing the Privacy and Security Challenges of the Internet of Things. *Journal of Internet Law*, *22*(4), 1–33.

Lee, S., & Kim, B. G. (2017). The impact of qualities of social network service on the continuance usage intention. *Management Decision*, *55*(4), 701–729.

Leu, J. (2010). *The benefit analysis of RFID use in the health management in the health management center—The experience in Shin Kong Wu Ho-Su Memorial Hospital*. National Taiwan University.

Luxton, D. D., Kayl, R. A., & Mishkind, M. C. (2012). mHealth data security: The need for HIPAA-compliant standardization. *Telemedicine Journal and e-Health*, *18*(4), 284–288.

Mabo, T., Swar, B., & Aghili, S. (2018, March). A Vulnerability Study of MHealth Chronic Disease Management (CDM) Applications (apps). In *World Conference on Information Systems and Technologies* (pp. 587-598). Springer.

Najera, P., Lopez, J., & Roman, R. (2011). Real-time location and inpatient care systems based on passive RFID. *Journal of Network and Computer Applications*, *34*(3), 980–989.

O'Loughlin, K., Neary, M., Adkins, E. C., & Schueller, S. M. (2019). Reviewing the data security and privacy policies of mobile apps for depression. *Internet Interventions: the Application of Information Technology in Mental and Behavioural Health*, *15*, 110–115.

Oetzel, M. C., & Spiekermann, S. (2014). A systematic methodology for privacy impact assessments: A design science approach. *European Journal of Information Systems*, *23*(2), 126–150.

Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., & Patsakis, C. (2018). Security and privacy analysis of mobile health applications: The alarming state of practice. *IEEE Access, 6*, 9390–9403.

Paul, D., Chi, H., & Allen, C. (2013, September). GPU-based simulation of wireless body area network. In *Proceedings of the 8th International Conference on Body Area Networks* (pp. 244-247). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

Pennic. (n.d.). *Accenture: Only 2% of Hospitals Engage Patients Using Mobile Apps*. HIT Consultant. Last accessed from https://hitconsultant.net/2016/01/06/31065/

Pournaghshband, V., Sarrafzadeh, M., & Reiher, P. (2013). Securing legacy mobile medical devices. In *Wireless Mobile Communication and Healthcare* (pp. 163–172). Springer.

Ranasinghe, Sheng, & Zeadally. (2010). *Unique Radio Innovation for the 21st Century: Building Scalable and Global RFID Networks.* Springer.

RFID in Health Care Presentations. (n.d.). *Case Study (DVD media).* http://www.rfidjournal.com/store/presentations/health-care on 11/9/2018

Section 74-2 of The Florida Administrative Code (FAC). (n.d.). https://www.flrules.org/gateway/ChapterHome.asp?Chapter=74-2

Sloane, E. B., & Gehlot, V. (2016). Improved population health surveillance and chronic disease management using secure email: Application of the DIRECT, IEEE 11073, HITSP, and IHE standards and protocols. *2016 18th Mediterranean Electrotechnical Conference (MELECON)*, 1-3.

Song, B., Hwang, J. Y., & Shim, K.-A. (2012). Security Improvement of an RFID Security Protocol of ISO/IEC WD 29167-6. *IEEE Communications Letters*, *15*(12), 1375–1377.

The JSON Data Interchange Syntax. (n.d.). *ECMA-404 Standard, 2nd Edition, December 2017*. http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-404.pdf

Ventola C. L. (2014). Mobile devices and apps for health care professionals: uses and benefits. *P & T: A Peer-Reviewed Journal for Formulary Management, 39*(5), 356–364.

Vulnerability Note, V. U. #176301. (n.d.). *Auto-Masking DCU 210E RP 210E and Marine Pro Observer App*. https://www.kb.cert.org/vuls/id/176301/

Vulnerability Note, V. U. #304725. (n.d.). *Bluetooth implementations may not sufficiently validate elliptic curve parameters during Diffie-Hellman key exchange*. https://www.kb.cert.org/vuls/id/304725/

Wallis, Blessing, Dalwai, & Shin. (2017). Integrating mHealth at point of care in low-and middle-income settings: The system perspective. *Global Health Action*, *10*(sup3).

Wessel, R. (n.d.). *Czech Hospital Using HF RFID to Track Chemotherapy Drugs*. http://www.rfidjournal.com/articles/view?3394/

West, D. M., & Bleiberg, J. (2014). *United States and China are Leading the M-Health Revolution, Brookings*. http://www.brookings.edu/blogs/techtank/posts/2014/03/14-us-china-leading-mHealth-revolution on 11/9/2018

World Health Organization. (2016). *Atlas of eHealth country profiles: The use of eHealth in support of universal health coverage*. https://apps.who.int/iris/bitstream/handle/10665/204523/9789241565219_eng.pdf;jsessionid=20E47D7679D5E7F6B2CDA13125A1132F?sequence=1

Yao, W., Chu, C., & Li, Z. (2012). The Adoption and Implementation of RFID Technologies in Healthcare: A Literature Review. *Journal of Medical Systems*, *36*(6), 3507–3525.

Yin, Y., Zeng, Y., Chen, X., & Fan, Y. (2016). The internet of things in healthcare: An overview. *Journal of Industrial Information Integration*, *1*, 3–13.

Zubaydi, F., Saleh, A., Aloul, F., & Sagahyroon, A. (2015, November). Security of mobile health (mHealth) systems. In *2015 IEEE 15th International Conference on Bioinformatics and Bioengineering (BIBE)* (pp. 1-5). IEEE.

Zornitza Genova Prodanoff is a senior member of the IEEE and professor at the University of North Florida. In 2016 her colleagues recommended her and she was awarded a Fidelity Information Services Distinguished Professor award for her and her students' contributions in scholarship. Her scientific work focuses on the design and performance of emerging wireless networks technologies and their application in the healthcare industry.

Cynthia Williams currently serves as an Associate Professor at the University of North Florida in Jacksonville, Florida. Dr. Williams is the program director for the Executive in Master of Health Administration Program, Co-Chair of the Research and Scholarship Committee and is a member of the Health Administration Advisory Board. As the Director for the Center for Aging Research, she is actively engaged with the community to support clinical and administrative applications of Telemedicine, E-health and mobile health applications. She has practical experience as a clinical using telemedicine and mobile applications. She has partnered with several community agencies to implement and evaluate programs that have employee advance technological solutions.

Hongmei Chi is Professor of the Department of Computer and Information Sciences at Florida A&M University. She has a broad base of research funding in scientific computation, cybersecurity, digital forensics, and data science. She teaches undergraduate and graduate courses in and network security and cryptography, and scientific computation. Her research interests span many areas related to parallel computing, mobile health security and cyber security. Her work in those areas has been published in top journals and conferences. She has been PI/ Co-PI of federal grants more than $2 million.