

2019

# An investigation of electronic Protected Health Information (e-PHI) privacy policy legislation in California for seniors using in-home health monitoring systems

Robert Lee Saganich

Nova Southeastern University, [robert.saganich@gmail.com](mailto:robert.saganich@gmail.com)

This document is a product of extensive research conducted at the Nova Southeastern University [College of Engineering and Computing](#). For more information on research and degree programs at the NSU College of Engineering and Computing, please click [here](#).

Follow this and additional works at: [https://nsuworks.nova.edu/gscis\\_etd](https://nsuworks.nova.edu/gscis_etd)

Part of the [Computer Sciences Commons](#)

## Share Feedback About This Item

---

### NSUWorks Citation

Robert Lee Saganich. 2019. *An investigation of electronic Protected Health Information (e-PHI) privacy policy legislation in California for seniors using in-home health monitoring systems*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (1075)  
[https://nsuworks.nova.edu/gscis\\_etd/1075](https://nsuworks.nova.edu/gscis_etd/1075).

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact [nsuworks@nova.edu](mailto:nsuworks@nova.edu).

An investigation of electronic Protected Health Information (e-PHI) privacy policy  
legislation in California for seniors using in-home health monitoring systems

by

Robert Saganich

A dissertation final report submitted in partial fulfillment of the requirements  
for the degree of Doctor of Philosophy  
in  
Information Assurance

College of Engineering and Computing  
Nova Southeastern University

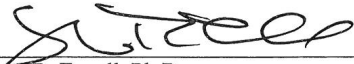
2019

We hereby certify that this dissertation, submitted by Robert Saganich, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.



Maxine S. Cohen, Ph.D.  
Chairperson of Dissertation Committee

4/23/2019  
Date



Steven R. Terrell, Ph.D.  
Dissertation Committee Member

4/23/2019  
Date



Yair Levy, Ph.D.  
Dissertation Committee Member

4/23/2019  
Date

Approved:



Meline Kevorkian, Ed.D.  
Interim Dean, College of Engineering and Computing

4/23/2019  
Date

College of Engineering and Computing  
Nova Southeastern University

2019

An Abstract of a Dissertation Final Report Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

An investigation of electronic Protected Health Information (e-PHI) privacy policy legislation in California for seniors using in-home health monitoring systems

by

Robert L. Saganich

April 2019

This study examined privacy legislation in California to identify those electronic Protected Health Information (e-PHI) privacy policies that are suited to seniors using in-home health monitoring systems. Personal freedom and independence are essential to a person's physical and mental health, and mobile technology applications provide a convenient and economical method for monitoring personal health. Many of these apps are written by third parties, however, which poses serious risks to patient privacy. Current federal regulations only cover applications and systems developed for use by covered entities and their business partners. As a result, the responsibility for protecting the privacy of the individual using health monitoring apps obtained from the open market falls squarely on the states.

The goal of this study was to conduct an exploratory study of existing legislation to learn what was being done at the legislative level to protect the security and privacy of users using in-home mobile health monitoring systems. Specifically, those developed and maintained by organizations or individuals not classified as covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The researcher chose California due to its reputation for groundbreaking privacy laws and high population of seniors.

The researcher conducted a content analysis of California state legislation, federal and industry best practices, and extant literature to identify current and proposed legislation regarding the protection of e-PHI data of those using in-home health monitoring systems.

The results revealed that in-home health monitoring systems show promise, but they are not without risk. The use of smartphones, home networks, and downloadable apps puts patient privacy at risk, and combining systems that were not initially intended to function together carries additional concerns. Factors such as different privacy-protection profiles, opt-in/opt-out defaults, and privacy policies that are difficult to read or are not adhered to by the application also put user data at risk.

While this examination showed that there is legislative support governing the development of the technology of individual components of the in-home health monitoring systems, it appears that the in-home health monitoring system as a whole is an immature technology and not in wide enough use to warrant legislative attention. In addition – unlike the challenges posed by the development and maintenance of the technology of in-home health monitoring systems – there is ample legislation to protect user privacy in mobile in-home health monitoring systems developed and maintained by those not classified as covered entities under HIPAA. Indeed, the volume of privacy law covering the individual components of the system is sufficient to ensure that the privacy of the system as a whole would not be compromised if deployed as suggested in this study. Furthermore, the legislation evaluated over the course of this study demonstrated consistent balance between technical, theoretical, and legal stakeholders.

This study contributes to the body of knowledge in this area by conducting an in-depth review of current and proposed legislation in the state of California for the past five years. The results will help provide future direction for researchers and developers as they struggle to meet the current and future needs of patients using this technology as it matures. There are practical applications for this study as well. The seven themes identified during this study can serve as a valuable starting point for state legislators to evaluate existing and proposed legislation within the context of medical data to identify the need for legislation to assist in protecting user data against fraud, identity theft, and other damaging consequences that occur because of a data breach.

## **Acknowledgements**

First and foremost, I wish to thank my beautiful wife and soulmate, Vicki. Your sacrifices, support, love, and understanding throughout these six years mean more to me than I can ever put into words. You are my biggest supporter and I could never have done this without you. I love you more every day.

To our daughter Ashley, thank you for the constant support and encouragement you have given me. It means more than you may realize.

To my dissertation chair, Dr. Maxine Cohen: Words cannot express my gratitude for the support and encouragement you provided as both an instructor and a mentor. You were always there for me when I needed guidance and direction and I could not have completed this process without you. You challenged me as both a student and a researcher, and the skills and lessons I learned from you will carry with me for the rest of my life. I am both proud and honored to have known you and to have had you as a mentor.

Thank you as well to my dissertation committee members, Dr. Steven Terrell and Dr. Yair Levy. The knowledge and insight you shared as instructors and advisors was invaluable to me throughout this journey and I am deeply grateful to you both for your support, wisdom, and guidance.

To my parents Richard and Ellen, thank you for the countless sacrifices you made and for instilling in me a strong work ethic and the drive to learn and to improve myself. To my brother Shawn, for always being there to listen and to help keep me grounded and focused on what is truly important in life. To my cousin Joe, thank you. Your presence in my life as a young man influenced me more profoundly than you can ever know.

## Table of Contents

<b>Abstract</b>	iii
<b>Acknowledgements</b>	v
<b>List of Tables</b>	viii
<b>List of Figures</b>	ix

## Chapters

### 1. Introduction 1

Background	1
Problem Statement	2
Dissertation Goal	3
Research questions	3
Relevance and Significance	4
Barriers and Issues	4
Assumptions, Limitations, and Delimitations	7
Definition of Terms	9
List of Acronyms	19
Summary	20

### 2. Review of the Literature 22

The evolution of patient monitoring systems	22
Privacy issues associated with in-home monitoring systems	26
Patient vulnerability and trust	28
Current federal regulations and regulatory bodies	29
Misinterpretation of regulations	31
Existing state legislation regarding protection of medical data	31
Summary	32

### 3. Methodology 35

Overview of research methodology/design	35
Research questions	38
Specific research method(s) to be employed	39
Institutional Review Board	39
Instrument development and validation	40
Sample	40
Data analysis	40
Formats for presenting results	40
Resource requirements	41
Summary	41

### 4. Results 43

Introduction	43
Data Collection	43

Results 45  
Summary 67

**5. Conclusions, Implications, Recommendations, and Summary 71**

Introduction 71  
Conclusions 71  
Limitations 74  
Implications 74  
Recommendations 76  
Summary 76

**Appendices**

A. IRB Approval 80  
B. Participant Questionnaire 82  
C. Interview Data 86  
D. Informed consent form 92  
E. Participant Request Email 96

**References 97**



## **List of Tables**

### **Tables**

1. List of potential participants and results 37
2. Number of hits for California by search term and legislative session 43
3. Number of bills by topic and year for California 44
4. Results 45

## **List of Figures**

### **Figures**

1. Population of seniors by state 6

## **Chapter 1**

### **Introduction**

#### **Background**

An increase in human life expectancy has resulted in a significant population of seniors (Ghose et al., 2013; Vuorimaa, Harmo, Hämäläinen, Itälä, & Miettinen, 2012). The World Health Organization predicts that the population of persons aged over 60 will grow from the current 650 million to over 2 billion by the year 2050 (Vuorimaa et al., 2012). Demands on personal caregivers and family members will increase as well, as current healthcare technology remains mainly limited to hospital, assisted living facilities, and hospice care. As healthcare costs skyrocket and resources become depleted, researchers are calling for the development of a new healthcare model that better addresses these concerns (Dickerson, Gorlin, & Stankovic, 2011; Vuorimaa et al., 2012). Extant literature shows that seniors prefer living at home rather than in a care facility (Vuorimaa et al., 2012). Medical monitoring and detection within the home would enhance the quality of life of the seniors and their families, and reduce the financial burden on the healthcare system (Alcalá, Parson, & Rogers, 2015; Dickerson et al., 2011; Sun, Fang, & Zhu, 2010; Vuorimaa et al., 2012). Personal freedom and independence are essential to a person's physical and mental health, and people of all ages are using mobile technology. mHealth applications are on the rise as well (Armontrout, Torous, Fisher, Drogin, & Gutheil, 2016). The IMS Institute for Healthcare Informatics reported in September 2015 that there were over 165,000 mHealth apps on the market, and the 2014 Health Information National Trends Survey reported 36% of adults had mHealth apps on their smartphones/tablets (Brzan, Rotman, Pajnkihar, & Klanjsek, 2016). As healthcare costs rise and healthcare infrastructure becomes

overburdened because of the population growth, it is imperative that mobile technologies continue to be leveraged to assist in independent living and in-home health monitoring of senior patients (Díaz-Bossini & Moreno, 2014; Reeder, Demiris, & Thompson, 2015). It is important, however, that the protection of patient data not be overlooked in the interest of technological advancement (Armontrout et al., 2016; Martínez-Pérez, de la Torre-Díez, & López-Coronado, 2014). The storage, forwarding, and access to personal health information of patients by unregulated third parties presents a massive potential for privacy loss for patients – and possibly family members and medical personnel, depending on how much information the database retains about a patient's relationships. Current federal regulations only cover applications and systems developed for use by covered entities and their business partners (Paul & Irvine, 2014; Yang & Silverman, 2014). As a result, the responsibility for protecting the privacy of the individual using health monitoring apps obtained from the open market falls squarely on the states.

## **Problem Statement**

More work is needed to protect the privacy of users' data that mobile applications collect, store, and transmit (Brzan et al., 2016; Martínez-Pérez et al., 2014; Varshney, 2014; Yang & Silverman, 2014). In particular, in-home health monitoring systems developed by individuals or organizations that existing federal regulations do not define as covered entities.

This study was originally designed as a two-state case study consisting of California, due to its reputation for groundbreaking privacy laws (Lovells, 2013; Willcox, 2017) and high population of seniors (U.S. Census Bureau, 2014); and Florida, because of the high percentage of seniors relative to the overall state population (U.S. Census Bureau, 2014). However, the

researcher was unable to obtain sufficient data on the state of Florida and had to change the study to a single-state case study consisting of California only.

### **Dissertation Goal**

The goal of this study was to conduct an exploratory study of existing legislation to learn what was being done at the legislative level to protect the security and privacy of users using in-home mobile health monitoring systems. Specifically, those developed and maintained by organizations or individuals not classified as covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

### **Research questions**

The main research question of this work was – what was the California state legislature doing to protect the security and privacy of users of in-home mobile health monitoring systems? Specifically, those developed and maintained by organizations or individuals not classified as covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)?

*RQ 1: What legislation did California have in place governing the development and maintenance of the technology used with mobile in-home health monitoring systems developed and maintained by organizations or individuals not classified as covered entities under HIPAA?*

*RQ2: What legislation did California have in place to protect the privacy of seniors using mobile in-home health monitoring systems developed and maintained by organizations or individuals not classified as covered entities under HIPAA?*

*RQ3: What was the required technical and legal expertise California needed to develop and enforce such legislation?*

### **Relevance and Significance**

Current literary guidance and regulations concerning privacy of mHealth applications is sparse and confusing, and researchers and clinicians alike are calling for more standardized guidance to enable developers, clinicians, and users to better leverage mHealth technology while preserving privacy and adhering to legal requirements (Armontrout et al., 2016; Health Information & the Law, 2016a; Lewis & Wyatt, 2014). This work explored existing and proposed California state legislation to learn what was being done to protect the privacy of user data collected, stored, and transmitted by systems or applications developed by entities not covered under existing federal regulations. Specifically, it addressed the risks to seniors relying on in-home health monitoring systems to provide maintenance and early warning of health problems.

This work will add to the body of knowledge and provide future directions for researchers and developers as they struggle to meet the current and future needs of patients using this technology.

### **Barriers and Issues**

The researcher anticipated three major barriers in conducting this study. The first was determining whom to interview. State websites list the current heads of agencies and other offices, but the actual work to create the legislation may have been done by researchers and presented to the state legislature. The number of perspectives involved was likely to make the identification of a starting point difficult. The researcher chose California due to its reputation

for groundbreaking privacy laws (Lovells, 2013; Willcox, 2017) and high population of seniors (See figure 1 for population data) (U.S. Census Bureau, 2014). The researcher conducted the literature review with the authors of the recommendation reports and research, and from there to the legislators who sponsored the bills.

The second major barrier was the number of people required to speak with to obtain the data. It was highly likely that no one person will be able to answer all the questions. The process would likely involve a long chain of sources, which would be a laborious and costly process with no clear end. For instance, since regulations evolve, and new regulations take their place, there would come a point where it would only be possible to go back so far in time before the necessary sources had retired, moved on to other locations, or were otherwise no longer available.

The third major barrier was whether the sources could and would participate. There may be professional reasons such as regulatory or legal constraints that prohibited the release of certain information to outside sources. Also, data and personnel compartmentalization might require input from numerous sources to get a complete picture. This may have prevented the researcher from gaining access to the requested information due to security concerns. There may also have been personal issues with the individual; they may have been unwilling to cooperate for whatever reason. Lack of a third-party introduction would also be a major problem, particularly given the popularity of social engineering attacks masquerading as students doing research.

Table 4-1.

**Population Aged 65 and Over Ranked by State: 2010**

(For information on confidentiality protection, nonsampling error, and definitions, see [www.census.gov/prod/cen2010/doc/sf1.pdf](http://www.census.gov/prod/cen2010/doc/sf1.pdf))

Population 65 and over			Percent 65 and over of state population		
Rank	State	Number	Rank	State	Percent
1	California . . . . .	4,246,514	1	Florida . . . . .	17.3
2	Florida . . . . .	3,259,602	2	West Virginia . . . . .	16.0
3	New York . . . . .	2,617,943	3	Maine . . . . .	15.9
4	Texas . . . . .	2,601,886	4	Pennsylvania . . . . .	15.4
5	Pennsylvania . . . . .	1,959,307	5	Iowa . . . . .	14.9
6	Ohio . . . . .	1,622,015	6	Montana . . . . .	14.8
7	Illinois . . . . .	1,609,213	7	Vermont . . . . .	14.6
8	Michigan . . . . .	1,361,530	8	North Dakota . . . . .	14.5
9	North Carolina . . . . .	1,234,079	9	Rhode Island . . . . .	14.4
10	New Jersey . . . . .	1,185,993	10	Arkansas . . . . .	14.4
11	Georgia . . . . .	1,032,035	11	Delaware . . . . .	14.4
12	Virginia . . . . .	976,937	12	Hawaii . . . . .	14.3
13	Massachusetts . . . . .	902,724	13	South Dakota . . . . .	14.3
14	Arizona . . . . .	881,831	14	Connecticut . . . . .	14.2
15	Tennessee . . . . .	853,462	15	Ohio . . . . .	14.1
16	Indiana . . . . .	841,108	16	Missouri . . . . .	14.0
17	Missouri . . . . .	838,294	17	Oregon . . . . .	13.9
18	Washington . . . . .	827,677	18	Arizona . . . . .	13.8
19	Wisconsin . . . . .	777,314	19	Massachusetts . . . . .	13.8
20	Maryland . . . . .	707,642	20	Michigan . . . . .	13.8
21	Minnesota . . . . .	683,121	21	Alabama . . . . .	13.8
22	Alabama . . . . .	657,792	22	Wisconsin . . . . .	13.7
23	South Carolina . . . . .	631,874	23	South Carolina . . . . .	13.7
24	Kentucky . . . . .	578,227	24	New Hampshire . . . . .	13.5
25	Louisiana . . . . .	557,857	25	New York . . . . .	13.5
26	Colorado . . . . .	549,625	26	Oklahoma . . . . .	13.5
27	Oregon . . . . .	533,533	27	Nebraska . . . . .	13.5
28	Oklahoma . . . . .	506,714	28	New Jersey . . . . .	13.5
29	Connecticut . . . . .	506,559	29	Tennessee . . . . .	13.4
30	Iowa . . . . .	452,888	30	Kentucky . . . . .	13.3
31	Arkansas . . . . .	419,981	31	New Mexico . . . . .	13.2
32	Mississippi . . . . .	380,407	32	Kansas . . . . .	13.2
33	Kansas . . . . .	376,116	33	Indiana . . . . .	13.0
34	Nevada . . . . .	324,359	34	North Carolina . . . . .	12.9
35	West Virginia . . . . .	297,404	35	Minnesota . . . . .	12.9
36	New Mexico . . . . .	272,255	36	Mississippi . . . . .	12.8
37	Utah . . . . .	249,462	37	Illinois . . . . .	12.5
38	Nebraska . . . . .	246,677	38	Wyoming . . . . .	12.4
39	Maine . . . . .	211,080	39	Idaho . . . . .	12.4
40	Hawaii . . . . .	195,138	40	Washington . . . . .	12.3
41	Idaho . . . . .	194,668	41	Louisiana . . . . .	12.3
42	New Hampshire . . . . .	178,268	42	Maryland . . . . .	12.3
43	Rhode Island . . . . .	151,881	43	Virginia . . . . .	12.2
44	Montana . . . . .	146,742	44	Nevada . . . . .	12.0
45	Delaware . . . . .	129,277	45	District of Columbia . . . . .	11.4
46	South Dakota . . . . .	116,581	46	California . . . . .	11.4
47	North Dakota . . . . .	97,477	47	Colorado . . . . .	10.9
48	Vermont . . . . .	91,078	48	Georgia . . . . .	10.7
49	Wyoming . . . . .	70,090	49	Texas . . . . .	10.3
50	District of Columbia . . . . .	68,809	50	Utah . . . . .	9.0
51	Alaska . . . . .	54,938	51	Alaska . . . . .	7.7

Source: U.S. Census Bureau, 2011a; 2010 Census.

Figure 1. Population of seniors by state.



## **Assumptions, Limitations, and Delimitations**

### *Assumptions*

In addition to information readily available on the Internet, this study required access to recorded data stored in local libraries and government records. It was assumed that these resources would be available and remain available throughout this study.

The researcher would also need to interview members of the state privacy office, its equivalent, or state legislators – either in person or via telephone or the web – to obtain clarification of facts or to obtain information not found elsewhere. It was assumed that the individuals needed to interview would remain available throughout this study.

In any study involving human subjects, the researcher must assume they will be truthful (Terrell, 2016). In the case of this study, there may have been professional reasons such as security, regulatory, or legal constraints that prohibited the release of certain information to outside sources. There may also have been personal issues with the individual; they may have been unwilling to cooperate for whatever reason. The researcher assumed the sources were able and willing to provide their full cooperation and would be truthful in their response.

### *Limitations*

The researcher used the Internet to gather the information pertinent to this study. New regulations are introduced every day, but the data gathering portion of the study was time-constrained.

The legislative process is ongoing, and there is often a good amount of turnover. As a result, it may only be possible to go back so far in time before the necessary sources have retired, moved on to other locations, or are otherwise no longer available. This could lead to an incomplete or inaccurate account of a piece of legislation.

### *Delimitations*

This study focused on California due to its reputation for groundbreaking privacy laws (Lovells, 2013; Willcox, 2017) and because it has the highest population of seniors in the country (U.S. Census Bureau, 2014).

This study was originally designed to examine legislation by gathering data obtained from both the state legislative websites and interviews with legislators involved in the legislation identified during the legislative search. This study originally included the state of Florida because it has the highest population of seniors relative to the overall population (U.S. Census Bureau, 2014). However, the Florida legislative website provided limited data relevant to this study, and the researcher was unable to locate a sufficient number of participants to interview. As a result, the researcher had to discard the data for Florida and change the study to a single-state case study focusing on California only. While the California legislative website provided an abundance of data, only two of the original respondents actually participated in the survey. This did not provide a sufficient sample size of participants to accurately represent the legislative body of California, and so the survey and interview data was discarded. The discarded data from the study (Instrument development and validation, Data analysis, Survey results, and Implications) are included in Appendix C.

The exclusion of the survey and interview data left only the data collected online, which is not suitable for a case study (Terrell, 2016). However, the data from the California legislative web site proved sufficient to address the research questions in this study on its own. In this case a content analysis is appropriate (Terrell, 2016), and so the researcher changed the study once again.

## Definitions of Terms

**Availability** – Data is accessible and usable when needed (Medicare learning network, 2016).

**Access** – California A.B. 32 (2015) defines *access* as “to gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network” (p. 2).

**Aggregate consumer information** – California S.B 1121 (2018) defines *aggregate consumer information* as:

information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. “Aggregate consumer information” does not mean one or more individual consumer records that have been deidentified. (p. 10)

California A.B. 375 (2018) discusses aggregate consumer information as well. The definition is the same as that listed here.

**Authentication** – California A.B. 1906 defines *authentication* as “a method of verifying the authority of a user, process, or device to access resources in an information system” (p. 2).

**Behavioral tracking** – The practice of collecting information about a user while they are using an application. Examples include personal data, browsing and purchase history, internet searches, ads a user clicks on or closes, and which type of media a user prefers to view or listen to (Sonam & Shubhangini, 2014).

**Biometric information** – California S.B. 1121 (2018) defines *biometric information* as:

an individual’s physiological, biological or behavioral characteristics, including an individual’s deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information (p. 10).

**Bot** – California S.B. 1001 (2018) defines a *bot* as “an automated online account on an online platform that is designed to mimic or behave like the account of a person” (p. 2).

**Breach of the security of the system** – California S.B. 570 (2015) defines *breach of the security of the system* as:

unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure (p. 4).

California A.B. 964 (2015) discusses breach of the security of the system as well. The definition is the same as that listed here.

**Caregiver** – California A.B. 1744 (2014) defines *caregiver* as “any relative, partner, friend, or neighbor who has a significant relationship with, and who provides a broad range of assistance to, an older person or an adult with a chronic or disabling condition” (p. 2). California A.C.R. 38 (2015) expands the definition of caregiver to include a spouse.

**Caretaker** – California A.B. 1718 (2016) defines *caretaker* as “any person who has the care, custody, or control of, or who stands in a position of trust with, an elder or a dependent adult” (p. 4). California A.B. 329 (2017) discusses caretakers as well. The definition is the same as that listed here.

**Cloud computing** – Mell and Grance (2011) define *cloud computing* as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (p. 2).

**Commercial health monitoring program** – California A.B. 2688 (2016) defines a *commercial health monitoring program* as “a commercial Internet Web site, online service, or product used

by consumers whose primary purpose is to collect the consumer's individually identifiable health monitoring information" (p. 3).

**Computer contaminant** – California A.B. 32 (2015) defines *computer contaminant* as:

any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network (p. 3).

**Computer network** – California A.B. 32 (2015) defines *computer network* as "any system that provides communications between one or more computer systems and input/output devices, including, but not limited to, display terminals, remote systems, mobile devices, and printers connected by telecommunication facilities" (p. 2).

**Computer program or software** – California A.B. 32 (2015) defines *computer program or software* as "a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions" (p. 2).

**Computer services** – according to California A.B. 32 (2015) *computer services* "includes, but is not limited to, computer time, data processing, or storage functions, Internet services, electronic mail services, electronic message services, or other uses of a computer, computer system, or computer network" (p. 2).

**Computer system** – California A.B. 32 (2015) defines a *computer system* as:

a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions, including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control (p. 2).

**Confidential communication** – California A.B. 1671 (2016) defines *confidential*

*communication* as:

any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made in a public gathering or in any legislative, judicial, executive, or administrative proceeding open to the public, or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded (p. 2).

**Confidentiality** – Ensures data are only made available to authorized entities (Medicare learning network, 2016).

**Connected device** – California A.B. 1906 (2018) defines *connected device* as “any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address” (p. 2).

**Data** – California A.B. 32 (2015) defines *data* as:

a representation of information, knowledge, facts, concepts, computer software, or computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device (p. 2).

**Data at rest** – with respect to data on a smartphone, California A.B. 1681 (2016) defines *data at rest* as “data that is parked, stored, and no longer in motion, such as pictures and text messages” (p. 3).

**Data broker** – California S.B. 1348 (2014) defines *data broker* as:

a commercial entity that collects, assembles, or maintains personal information concerning individuals residing in California who are not customers or employees of that entity ... for the purposes of selling or offering for sale, or other consideration, the personal information to a third party (p. 3).

**Deidentified** – California S.B. 1121 (2018) defines *deidentified* as:

information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

- Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
- Has implemented business processes that specifically prohibit reidentification of the information.
- Has implemented business processes to prevent inadvertent release of deidentified information.
- Makes no attempt to reidentify the information (p. 12).

**Dependent adult** – California A.B. 1718 (2016) defines a *dependent adult* as:

any person who is between the ages of 18 and 64, who has physical or mental limitations which restrict his or her ability to carry out normal activities or to protect his or her rights, including, but not limited to, persons who have physical or developmental disabilities or whose physical or mental abilities have diminished because of age. “Dependent adult” includes any person between the ages of 18 and 64 who is admitted as an inpatient to a 24-hour health facility (p. 4).

California A.B. 329 (2017) discusses dependent adults as well. The definition is the same as that listed here.

**Digital health feedback system** – California A.B. 2167 (2018) defines *digital health feedback system* as:

an ingestible sensor that collects or sends information about an individual, and is used in conjunction with either, or both, of the following:

- A sensor or device placed inside or worn on the body that collects or sends information about an individual.
- A software platform that is connected to the Internet, directly or indirectly, or to another device that receives and displays information collected or sent from a sensor or device as described in paragraph (1) (p. 3).

**Elder** – California A.B. 1718 (2016) defines *elder* as “any person who is 65 years of age or older” (p. 4). California A.B. 329 (2017) discusses elders as well. The definition is the same as that listed here.

**Electronic means** – California A.B. 695 (2015) defines *electronic means* to “include opening an email account or an account or profile on a social networking Internet Web site in another person’s name” (p. 2).

**Electronic mail** – California A.B. 32 (2015) defines *electronic mail* as:

an electronic message or computer file that is transmitted between two or more telecommunications devices; computers; computer networks, regardless of whether the network is a local, regional, or global network; or electronic devices capable of receiving electronic messages, regardless of whether the message is converted to hard copy format after receipt, viewed upon transmission, or stored for later retrieval (p. 3).

**Encrypted** – California A.B. 2828 (2016) defines *encrypted* as “rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security” (p. 5). California A.B. 2182 (2018) and California A.B. 2678 (2018) use the same definition of *encrypted* as that listed here.

**Geolocation information** – California A.B. 83 (2016) defines *geolocation information* as:

location data generated by a consumer device capable of connecting to the Internet that directly identifies the precise physical location of the identified individual at particular times and that is compiled and retained. “Geolocation information” does not include the contents of a communication or information used solely for 911 emergency purposes (p. 3).

**Government computer system** – California A.B. 32 (2015) defines *government computer system* as “any computer system, or part thereof, that is owned, operated, or used by any federal, state, or local governmental entity” (p. 2).

**Health insurance information** – California A.B. 2828 (2016) defines *health insurance information* as “an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records” (p. 5). California A.B. 2182 (2018) and California A.B. 2678 (2018) use the same definition of *health insurance information* as that listed here.

**Health monitoring information** – California A.B. 2688 (2016) defines *health monitoring information* as:



information, in electronic or physical form, about a consumer's mental or physical condition that is collected by a commercial health monitoring program through a direct measurement of a consumer's mental or physical condition or through user-input regarding a consumer's mental or physical condition into a commercial health monitoring program (p. 3).

**Homepage** – California S.B 1121 (2018) defines *homepage* as:

the introductory page of an Internet Web site and any Internet Web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information," or settings page, and any other location that allows consumers to review [a required notice] before downloading the application (p. 13).

**Individually identifiable** – California A.B. 2688 (2016) defines *individually identifiable* as:

information *that* [*sic*] includes or contains an element of personal identifying information sufficient to allow identification of the consumer, including, but not limited to, the consumer's name, address, electronic mail address, telephone number, social security number, or unique electronic identifier, or other information that, alone or in combination with other publicly available information, reveals the consumer's identity (p. 4).

**Individually identifiable health information** – The HIPAA Privacy Rule defines *Individually identifiable health information* as:

Information that can either identify an individual or be reasonably believed to identify an individual. PHI falls into three categories: past, present or future physical or mental health or condition; details about the healthcare to the individual; or the past, present, or future payment for healthcare to the individual. Examples include name, address, birth date, and Social Security Number (U.S. Department of Health and Human Services, 2003, p. 4).

**Integrity** – Ensures data is not destroyed or manipulated by other than authorized means or persons (Medicare learning network, 2016).

**Internet domain name** – California A.B. 32 (2015) defines *Internet domain name* as "a globally unique, hierarchical reference to an Internet host or service, assigned through centralized Internet naming authorities, comprising a series of character strings separated by periods, with the rightmost character string specifying the top of the hierarchy" (p. 3).

**Manufacturer** – California A.B. 1906 defines *manufacturer* as:

the person who manufactures, or contracts with another person to manufacture on the person's behalf, connected devices that are sold or offered for sale in California. ... a contract with another person to manufacture on the person's behalf does not include a contract only to purchase a connected device, or only to purchase and brand a connected device (p. 3).

**Online** – California S.B. 1001 (2018) defines *online* as “appearing on any public-facing Internet Web site, Web application, or digital application, including a social network or publication” (p. 2).

**Online platform** – California S.B. 1001 (2018) defines *online platform* as “any public-facing Internet Web site, Web application, or digital application, including a social network or publication” (p. 2).

**Operator** – California S.B. 576 (2015) defines *operator* as:

any person or entity that owns an Internet Web site or an online service, including a mobile application, that collects and maintains personally identifiable information from a consumer residing in California who uses or visits the Internet Web site or online service if the Internet Web site or online service is operated for commercial purposes. It does not include any third party that operates, hosts, or manages, but does not own, an Internet Web site or online service on the owner's behalf or by processing information on behalf of the owner (p. 3).

**Privacy** – California H.R. 10 (2017) defines *privacy* as “the recognition that a free and democratic society respects the autonomy of individuals to choose the circumstances and degree to which individuals will expose their personal characteristics, attitudes, and behavior” (p.1).

**Profile** – California A.B. 32 (2015) defines *profile* to mean either:

- A configuration of user data required by a computer so that the user may access programs or services and have the desired functionality on that computer.
- An Internet Web site user's personal page or section of a page that is made up of data, in text or graphical form, that displays significant, unique, or identifying information, including, but not limited to, listing acquaintances, interests, associations, activities, or personal statements (p. 3).

**Protected Health Information (PHI)** – The HIPAA Privacy Rule defines *Protected Health Information (PHI)* as “‘individually identifiable health information’ held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral” (U.S. Department of Health and Human Services, 2003, p. 3).

**Public safety infrastructure computer system** – California A.B. 32 (2015) defines *public safety infrastructure computer system* as:

any computer system, or part thereof, that is necessary for the health and safety of the public including computer systems owned, operated, or used by drinking water and wastewater treatment facilities, hospitals, emergency service providers, telecommunication companies, and gas and electric utility companies (p.2).

**Ransomware** – California S.B. 1137 (2016) defines *ransomware* as:

a computer contaminant ... or lock placed or introduced without authorization into a computer, computer system, or computer network that restricts access by an authorized person to the computer, computer system, computer network, or any data therein under circumstances in which the person responsible for the placement or introduction of the ransomware demands payment of money or other consideration to remove the computer contaminant, restore access to the computer, computer system, computer network, or data, or otherwise remediate the impact of the computer contaminant or lock (p. 2).

**Security feature** – California A.B. 1906 defines *security feature* as “a feature of a device designed to provide security for that device” (p. 2).

**Smartphone** – California S.B. 962 defines *smartphone* as:

a cellular radio telephone or other mobile voice communications handset device that includes all of the following features:

- Utilizes a mobile operating system.
- Possesses the capability to utilize mobile software applications, access and browse the Internet, utilize text messaging, utilize digital voice service, and send and receive email.
- Has wireless network connectivity.
- Is capable of operating on a long-term evolution network or successor wireless data network communication standards (p. 2).

**Social media** – California A.B. 1671 (2016) defines *social media* as “an electronic service or account, or electronic content, including, but not limited to, videos or still photographs, blogs,

video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations” (p. 3).

**Sold in California** – according to California S.B. 962, *sold in California*:

or any variation thereof, means that the smartphone is sold at retail from a location within the state, or the smartphone is sold and shipped to an end-use consumer at an address within the state. “Sold in California” does not include a smartphone that is resold in the state on the secondhand market or that is consigned and held as collateral on a loan (p. 2).

**Supporting documentation** – according to California A.B. 32 (2015), *supporting documentation*:

includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software (p. 2).

**Trusted system** – California A.B. 22 (2017) defines a *trusted system* as “a combination of technologies, policies, and procedures for which there is no plausible scenario in which a document retrieved from or reproduced by the system could differ substantially from the document that is originally stored” (p. 2). California A.B. 2225 (2018) modifies this definition to change “document” to “public record” (p. 4).

**Unauthorized access, destruction, use, modification, or disclosure** – California A.B. 2167 (2018) defines *unauthorized access, destruction, use, modification, or disclosure* as “access, destruction, use, modification, or disclosure that is not authorized by the person about whom the information pertains unless the access, destruction, use, modification, or disclosure is authorized or required by law” (p. 7).

**Victim expenditure** – California A.B. 32 (2015) defines *victim expenditure* as “any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system,

computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access” (p. 3).

### **List of Acronyms**

<b>ADHD</b>	<b>Attention-Deficit/Hyperactivity Disorder</b>
<b>BSN</b>	<b>Body Sensor Network</b>
<b>COTS</b>	<b>Commercial off-the-shelf</b>
<b>ECG</b>	<b>Electrocardiogram</b>
<b>EEG</b>	<b>Electroencephalogram</b>
<b>EMG</b>	<b>Electromyogram</b>
<b>Empath</b>	<b>Emotional Monitoring for PATHology</b>
<b>e-PHI</b>	<b>electronic Protected Health Information</b>
<b>GSR</b>	<b>Galvanic Skin Response</b>
<b>HIPAA</b>	<b>Health Insurance Portability and Accountability Act of 1996</b>
<b>HITECH</b>	<b>Health Information Technology for Economic and Clinical Health</b>
<b>IRB</b>	<b>Institutional Review Board</b>
<b>LED</b>	<b>Light-Emitting Diode</b>
<b>mHealth</b>	<b>Mobile Health</b>
<b>PHI</b>	<b>Protected Health Information</b>
<b>PII</b>	<b>Personally identifiable information</b>
<b>SDK</b>	<b>Software Development Kit</b>
<b>TOS</b>	<b>Terms of Service</b>
<b>UbiHeld</b>	<b>Ubiquitous Healthcare for the Elderly</b>

## Summary

People are living longer, and the impact on our healthcare infrastructure is becoming critical (Dickerson et al., 2011; Vuorimaa et al., 2012). As healthcare costs skyrocket and resources become depleted, researchers are calling for a new way to care for the needs of the aging population (Reeder et al., 2015; Vuorimaa et al., 2012). Medical monitoring and detection within the home would enhance the quality of life of seniors and their families and reduce the financial burden on the healthcare system (Alcalá et al., 2015; Dickerson et al., 2011; Sun et al., 2010; Vuorimaa et al., 2012). Personal freedom and independence are essential to a person's physical and mental health, and mobile technology applications provide a convenient and economical method for monitoring personal health. Many of these apps are written by third parties, however, which poses serious risks to patient privacy. Current federal regulations only cover applications and systems developed for use by covered entities and their business partners. As a result, the responsibility for protecting the privacy of the individual using health monitoring apps obtained from the open market falls squarely on the states. The goal of this study was to conduct an exploratory study of existing legislation to learn what was being done at the legislative level to protect the security and privacy of users using in-home mobile health monitoring systems. Specifically, those developed and maintained by organizations or individuals not classified as covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

This study was originally designed as a two-state case study consisting of California and Florida. The Florida legislative website provided limited data relevant to this study, and the researcher was unable to locate a sufficient number of participants to interview. As a result, the researcher had to discard the data for Florida and change the study to a single-state case study

focusing on California only. While the California legislative website provided an abundance of data, only two of the original respondents actually participated in the survey. This did not provide a sufficient sample size of participants, and so the survey and interview data were discarded (see Appendix C). As a result, the researcher had to abandon the case study approach in favor of the exploratory study consisting of California legislation.

## Chapter 2

### Review of the Literature

Six themes emerged during the review of the literature: the evolution of patient monitoring systems; privacy issues associated with in-home monitoring systems; patient vulnerability and trust; current federal regulations and regulatory bodies; misinterpretation of regulations; and existing state legislation regarding the protection of medical data. A literature review section on each topic follows.

#### *The evolution of patient monitoring systems*

The earliest and most resilient patient monitoring system is the Body Sensor Network (BSN). These systems consist of tiny sensors worn on or implanted in the patient's body. These sensors gather information about the patient's current physical health and transmit it to a provider or other entity (Caldeira, Rodrigues, & Lorenz, 2012; Shu-Di, Yuan-Ting, & Lian-Feng, 2005; Sun et al., 2010). Many applications within the healthcare industry use these systems. BSNs in hospitals and other live-in facilities provide real-time patient information to medical staff (Caldeira et al., 2012). Also, both COTS and proprietary solutions are used to detect falls, monitor physical and neurological activity, and track physiological data such as heart activity and blood oxygenation (Calhoun et al., 2012). BSNs also help medication regimens by controlling insulin pumps and dispensing medications (Calhoun et al., 2012; Hanson et al., 2009). BSNs are being used to control prosthetic devices and providing sensory stimulation for the hearing or visually impaired (Calhoun et al., 2012). BSNs can be so small that they can be implanted into the eye – as in the intraocular pressure sensor for glaucoma treatment, or embedded into a contact lens to monitor glucose levels in diabetic patients (Calhoun et al., 2012).



The value of BSNs in the home health-monitoring environment is undeniable (Calhoun et al., 2012; Sun et al., 2010). However, these systems are highly specialized, and this brings drawbacks and disadvantages. For instance, the costs associated with regulatory compliance, development, manufacturing, marketing, and training can quickly add up (Hanson et al., 2009). Companies would either have to mass-produce a system designed to a single application or develop less-specialized systems to permit cross-application compatibility (Hanson et al., 2009).

As the patient monitoring industry grew, manufacturers and researchers began to explore the possibility of leveraging existing technology such as smartphones to build their systems. Lee et al. (2015) developed an in-home system for tracking a user's location using only a smartphone and a smartwatch. They reasoned that since users do not always carry their smartphone while they are in their home, the microphone and inertial sensors on the smart watch could be used to generate what they called "activity fingerprints," which could then be used to estimate the user's location in the house. The advantage of the system was that it eliminates the need for additional infrastructure, sensors, and user training that in-home tracking systems often require. The UbiHeld system developed by Ghose et al. (2013) leveraged multiple existing technologies to create their system for monitoring the physical and mental well-being of seniors. Multiple Microsoft Kinect systems deployed throughout the home provided skeletal tracking of the user, while social media activity provided a perspective of the user's mental state. The data was transferred and stored on a backend server for storage and processing. A key benefit of this system was the skeletal tracking afforded by the Microsoft Kinect systems did not compromise the user's privacy since there was no actual video or image of the user. Dickerson et al. (2011) developed a system called Empath to monitor symptoms of depressive episodes. Their system used a variety of components: a central Web server/database, independent tri-axis accelerometers

attached to the patient's bed to monitor sleep patterns, a wireless body weight scale to monitor symptoms of changing eating habits, motion detectors and door/window contact switches to detect movement within the house, and a microphone attached to a touchscreen device to monitor speech patterns. The system transmitted the data to the Web server, which ran all analysis routines at preset intervals. The authors cited research estimating that over 15% of seniors had depressive episodes and posited that the effects of living alone longer due to technological advancements would exacerbate this problem. They proposed future research using seniors living alone as a target group. Alcala et al. (2015) analyzed data from smart electricity meters to identify a patient's activities by evaluating the electricity usage of an appliance. They tested the usage of a kettle in 13 UK homes to see if their algorithm could successfully detect usage patterns. They found their system successfully detected usage over 80% of the time with less than 10% false positives. Considering these results, they plan to expand their system to identify other appliances in use and to expand the research to include other countries where such technology is viable.

As the potential applications of in-home monitoring systems continued to grow, people began to realize the need to cut down on cost, user training, and expensive and specialized support requirements. Given the success of earlier systems in leveraging existing technology (Lee et al., 2015), researchers began to evaluate existing products never intended for medical applications, such as gaming systems. These systems had become so advanced over the years that they had much of the technology and sensors already built into them.

Dhillon, Ramos, Wünsche, and Lutteroth (2012) examined four such popular devices for their potential application to the health monitoring industry. The first device was the Nintendo Wii remote — the main controller for Nintendo's Wii console. It features motion-sensing ability, a

three-axis accelerometer, a high-resolution/high-speed infrared camera, and Bluetooth connectivity. The device provides audio, visual, and tactile feedback to the user via speakers, vibration, and LEDs. While initially intended for gaming applications, this device has already seen success in health monitoring and physical rehabilitation scenarios where the device was physically attached to the patients. The main drawback to this approach was discomfort or disruption to the user's daily routine.

The second device examined was the Sony PlayStation Move — the controller for Sony's PS3 console. It offers a three-axis gyroscope, a three-axis accelerometer, a terrestrial magnetic field sensor, vibration feedback, and Bluetooth connectivity. An SDK called "Move.me" provides the ability to write custom code. Unlike other systems, however, the device and computer must be plugged into the console. While the higher precision of the system is useful for games, it could cause frustration for users in medical applications because small gestures such as tremors or shaking could be captured and interpreted as input by the system. Also, a properly lit environment is required for the device to work; if the room is too dark, it will cause reflections on the screen. If it is too bright, the camera can have problems picking up images.

The third device was the Webcam. Webcams can provide an efficient and cost-effective method for maintaining communications between patients and healthcare professionals. Webcams come as standard equipment on many desktop and laptop computers, and external Webcams can be purchased relatively inexpensively and connected to the computer if it does not have one via USB connection. Studies have shown that some patients find this medium preferable because it delivers the doctor/patient interaction experience without the distractions of the office setting or the inconvenience of having to travel to the office. This type of medium can

also prove helpful for patients who are working through social phobias since there is no contact with other persons and situations that would cause them anxiety.

The last device was Microsoft's Kinect — the input device for the Microsoft Xbox 360. The user interacts with the console via voice, gestures, and body movements. The device contains a Webcam, an infrared laser, a sensor system, and a microphone. The SDK provides for detection of human outlines, skeletal tracking, and facial recognition. The device connects directly to the computer via USB, so no special connections are required. The only drawback is the requirement for a well-lit and unobstructed environment, which could prove troublesome in a small apartment or cramped space. The Kinect has proven beneficial in physical rehabilitation scenarios because the user is not required to wear sensors or stand or sit in a fixed position, which makes it ideal for patients in wheelchairs. The motion-tracking feature has also proven useful in studies involving patients with ADHD and autism.

#### *Privacy issues associated with in-home monitoring systems*

In-home health monitoring systems allow seniors to enjoy a higher quality of life by living longer in their homes. In the past, specialized companies dedicated solely to the healthcare industry were the only source for these systems. Today's systems use smartphones, home wireless networks, and downloadable apps to collect, store, and transmit patient status and data to family members, private caregivers, and medical professionals in real-time (Jiya, 2016; Paul & Irvine, 2014). While these systems provide an efficient and effective method for monitoring the patient status and alerting healthcare professionals and family members, they may also put the patient privacy at risk (Al Ameen, Liu, & Kwak, 2012; Avancha, Baxi, & Kotz, 2012; Jiya, 2016). These applications are developed and marketed in the global market, which is largely unregulated. Patient data could be stored anywhere, retained forever, and shared or sold at the

will of the app owner. Indeed, Paul and Irvine (2014) found such statements explicitly stated in the privacy and user agreements in several popular health monitoring services.

Health apps and systems can pose significant threats to patient privacy. Of particular concern is the compromise of patient information caused by the interaction of dissimilar systems with incompatible privacy protection profiles (Calhoun et al., 2012). Because these systems collect data from so many different sources it may seem harmless but each source has a different privacy policy or protection profile, and the combination of the data could exceed the privacy protection afforded by the application (Ammar, Malik, Rezgui, & Alodib, 2014). Still another concern is default opt-in/opt-out settings, which are often framed by the developer to permit sharing of user information by defaulting to "yes" (Bellman, Johnson, & Lohse, 2001).

Privacy and security policies should be easy for users to understand (Rowan & Dehlinger, 2014; Shneiderman et al., 2016). However, Terms of Service (TOS), permissions requirements, and privacy policies often employ such small fonts and complex language that they can be tough to read (Burkell & Fortier, 2013a; Bustos-Jiménez, 2014). In their study, Rowan and Dehlinger (2014) found that the average privacy policy was written above the 12th-grade level and was an average of 4.8 pages long. By contrast, the recommended writing level for health or safety instruction documents is the 5th grade, and documents for the general public is the 9th grade.

Another concern is that privacy policies do not always accurately represent the behavior of the application. For instance, Njie (2016) found that only about 50% of the apps analyzed posted a privacy policy and adhered to it. Other studies have shown that some apps have no policy at all, or the app's privacy policy did not mention such items as behavioral tracking, third-party sharing policies, and data retention and ownership (Paul & Irvine, 2014; Rowan & Dehlinger, 2014).

Another concern with privacy policies concerns the retrieval of multiple items of a person's EHR

from several apps on the person's phone. Even if each piece of data gathered is within the privacy policy of the app providing it, the aggregate data may provide more of the EHR than intended or acceptable (Ammar et al., 2014).

Also, it seems that apps with the most detailed privacy policies often pose some of the greatest privacy risks (Ackerman, 2016). This suggests that privacy policies are written primarily to protect the company rather than the user, purposely doing so in a way that's difficult for the average user to understand (Njie, 2016).

#### *Patient vulnerability and trust*

A person's medical records contain an extensive amount of deeply personal information, collected over the course of their life (Rindfleisch, 1997; Wen & Tarn, 2006). A person's record might include such information as dietary habits, sexual orientation, history of diseases, medications, family history, laboratory test results, x-rays, and a host of other data (Choi, Capitan, Krause, & Streeper, 2006). In the past, such information was maintained in paper records in hospitals and doctors' offices, which were kept securely locked and accessible only by select personnel (Choi et al., 2006). While automation was initially intended to reduce paper processing and increase efficiency, today's health system could not survive without it (Choi et al., 2006; Rindfleisch, 1997). However, information technology and the related devices used to store, process, and transmit vital medical information pose serious threats to patient privacy. While individuals may feel comfortable with families knowing certain details of their medical condition, they will certainly not consider it appropriate for release to the public (Al Ameen et al., 2012). In addition to causing the patient embarrassment, it could also affect their lives in other ways. For instance, evidence of pre-existing conditions or personal conduct and habits could make it difficult to obtain employment, insurance, or other types of aid (Rindfleisch, 1997;

Sun et al., 2010; Wen & Tarn, 2006). A patient may be discriminated against for having certain types of illnesses and may be charged more for services based on the information contained in the record. In extreme cases, location tracking could be used to harm the individual physically (Jiya, 2016). As a result, patients may lie or omit details when talking with their doctor out of fear of the consequences of a possible breach (Choi et al., 2006; Wen & Tarn, 2006).

#### *Current federal regulations and regulatory bodies*

Before the passage of HIPAA, there was little federal legislation to protect patient privacy. Individual states were on their own when it came to the issue of personal privacy protection. At the time of HIPAA, only 30 states identified invasion of privacy as a punishable offense, and there was no uniformity among any of the states (Baumer, Earp, & Payton, 2000).

HIPAA was implemented to protect patient data but does not apply to everyone collecting or storing a patient's information. Health plans, healthcare clearinghouses, and healthcare providers who conduct certain financial and administrative transactions electronically are referred to as “covered entities” under the act and are the only ones accountable (U.S. Department of Health and Human Services, 2003). The Act has undergone many improvements over the years, the most recent being the HIPAA Omnibus Rule of 2013. This rule strengthened HIPAA in many ways, such as making business associates of covered entities liable for compliance. Also, it strengthened the limitations on the use and disclosure of PHI for marketing and fundraising purposes and adopted the HITECH Act enhancements to the Enforcement Rule (Leyva, 2013). However, the rule does not include entities that collect data from users via smartphone apps or wearable monitoring systems not developed for use specifically for or by a covered entity or business partner, meaning that such entities are exempt from regulation (Paul & Irvine, 2014). The responsibility of protecting patient's privacy lies squarely in the hands of the patient (when

choosing to provide their information to a third-party to use their app) and the privacy laws of the individual state where the patient lives.

When it comes to regulatory agencies, the American Health Information Management Association identifies five most likely to have the greatest impact on mobile health apps going forward (Yang & Silverman, 2014): The National Institute of Standards and Technology, The Federal Communications Commission, The Office for Civil Rights of the Department of Health and Human Services (HHS), The Federal Trade Commission (FTC), and the U.S. Food and Drug Administration.

The National Institute of Standards and Technology is not a regulatory body, but it can issue guidance on standards for technology such as mobile devices and software. The Federal Communications Commission reserves the 608-614 MHz, 1395-1400MHz, and 1427-1432MHz ranges for wireless medical telemetry (Federal Communications Commission, 2017). The Office for Civil Rights of the Department of Health and Human Services (HHS) monitors HIPAA violations, and the Federal Trade Commission (FTC) regulates false or deceptive advertising (Yang & Silverman, 2014). The U.S. Food and Drug Administration has released detailed guidance on the specific subset of mobile medical apps over which it intends to enforce its authority (U.S. Department of Health and Human Services Food and Drug Administration, 2015; Yang & Silverman, 2014). It details which mobile apps are considered medical devices and which are not. Also, it provides examples of current regulations, regulatory, requirements, and provides a frequently asked questions and additional resources section to aid marketers and developers (U.S. Department of Health and Human Services Food and Drug Administration, 2015). While the guidance documents are not enforceable, manufacturers still tend to follow them to prevent action by the FDA and consumer complaints (Yang & Silverman, 2014).



### *Misinterpretation of regulations*

Today's software developers are required to navigate a plethora of laws and regulations when designing their systems (Choi et al., 2006). As companies attempt to conform to these requirements, they must take care not to create security policies that are so convoluted and riddled with legalese that they end up confusing the employees and hampering their work efforts (Shneiderman et al., 2016). Healthcare providers, insurance companies, and attorneys alike have interpreted HIPAA differently, making it tough to ensure complete compliance (Varshney, 2007). Many violations are believed to be the result of how companies interpret regulations within the context of their business environment and information systems. Unfortunately, organizations are liable in case of violation of regulations regardless of the accuracy of their interpretation of the regulation or intent to comply (Breux & Anton, 2008).

Patients can misinterpret regulations as well. The U.S. Food and Drug Administration's definition of a "medically regulated device" can be confusing, causing consumers to mistakenly believe an app labeled as "medical" is provided by medical professionals or contains the appropriate privacy and security measures required by federal regulations (Brzan et al., 2016).

### *Existing state legislation regarding protection of medical data*

Many states have gone beyond federal standards by installing and maintaining health IT infrastructure and enacting legislation to further enhance the security and privacy of patient data (2016b). Such regulations permit states to tailor the protection of their residents to a more stringent level than that provided by federal regulations for providers doing business within their state. Some examples include the maintenance of medical records, what medical records must include, privacy and confidentiality, requirements for disclosure of personal health information (to whom and for what purpose) (2016b).

Currently, 20 states have laws to deal with the collection and treatment of patient data and records. While there is no clear uniformity among the states, there are some similarities (Health Information & the Law, 2016b). The passage of the California Online Privacy Protection Act of 2003 set the state of California apart as the first state in the United States to require commercial websites to post privacy policies if they collect Personally Identifiable Information (PII) from a person in California (Cooley Godward, 2016). California also leads the way with state laws often more stringent than HIPAA in 15 categories (Health Information & the Law, 2016b).

## **Summary**

Patient monitoring systems have evolved significantly over time. BSNs consisting of tiny sensors on or in the body have been used for many years in the healthcare field to provide real-time data to medical staff (Caldeira et al., 2012). They have evolved to provide everything from patient ambulatory status, vital signs (Calhoun et al., 2012), and control devices such as insulin pumps (Calhoun et al., 2012; Hanson et al., 2009). They are also being used to control prosthetic devices and assist the hearing and visually impaired (Calhoun et al., 2012). While these systems can provide invaluable assistance in the home monitoring system, they tend to be highly specialized, which results in high cost and limited ability to port to other systems (Hanson et al., 2009).

Manufacturers and researchers recognized this problem and began to explore ways to leverage existing technology. Lee et al. (2015) employed a smartphone and smartwatch to estimate a user's location within the home. Ghose et al. (2013) employed multiple Microsoft Kinect systems throughout a user's house to monitor their physical and mental status. Another approach was to monitor a user's activity by analyzing electrical appliance usage in the house to

identify what the user was doing throughout the day (Alcalá et al., 2015). Gesture, facial recognition, and movement recognition elements in gaming systems examined by Dhillon et al. (2012) showed promise in the areas of physical rehabilitation, home communication with caregivers and doctors for patients for whom travel was uncomfortable or otherwise difficult, and the treatment of social phobias by reducing the need for interaction with the external environment.

While these systems show promise in the home monitoring environment, they are not without risk. The use of smartphones, home networks, and downloadable apps put patient privacy at risk (Jiya, 2016). The combination of systems that were not initially intended to function together as a single system carries additional concerns. Different privacy protection profiles (Calhoun et al., 2012), opt-in/opt-out defaults (Bellman et al., 2001) and privacy policies that are difficult to read (Burkell & Fortier, 2013b; Bustos-Jiménez, 2014) or are not adhered to by the application (Njie, 2016) can put user data at risk.

While HIPAA was implemented to protect patient data, only covered entities (health plans, healthcare clearinghouses, and healthcare providers who conduct certain financial and administrative transactions electronically) are accountable under the act (U.S. Department of Health and Human Services, 2003). The HIPAA Omnibus Rule of 2013 expanded the definition of a covered entity to include business associates of covered entities, tightened down the use and disclosure of PHI for marketing and fundraising, and adopted the HITECH Act enhancements to the Enforcement Rule (Leyva, 2013). However, only covered entities and business partners are accountable (Paul & Irvine, 2014).

The current legislation is complex in both language and scope. Developers may never be fully confident that they are in compliance (Varshney, 2007) due to different interpretations of the

regulations, and users may incorrectly assume that a device or app is protected under federal regulations because the FDA labeled it a “medically regulated device” or a “medical app” (Brzan et al., 2016).

Some states have already begun passing legislation to protect patient data at a level beyond what federal regulations require. While some similarities exist, there is no uniformity across states regarding such protection (Health Information & the Law, 2016b).

## **Chapter 3**

### **Methodology**

#### **Overview of research methodology/design**

This study examined privacy legislation in California. The specific focus was in-home mobile health monitoring systems developed and maintained by organizations or individuals not classified as covered entities under HIPAA. The focus of this study was to identify what California was doing to protect the privacy of seniors – specifically those using in-home health monitoring systems.

This study was originally designed to examine legislation by gathering data from the state legislative websites and interviews with legislators involved in the legislation identified during the legislative search. The original study also called for a two-state case study consisting of California, due to its reputation for groundbreaking privacy laws (Lovells, 2013; Willcox, 2017) and high population of seniors (U.S. Census Bureau, 2014); and Florida, because of the high percentage of seniors relative to the overall state population (U.S. Census Bureau, 2014). The researcher was able to find an abundance of legislative data on California on their website, but the Florida legislative website provided limited data relevant to this study. Furthermore, finding legislators to interview proved an additional challenge. The researcher identified a total of 18 legislators – eight from California and 10 from Florida – to interview based on the analysis of the legislation gathered from the state websites and committee membership. While this initially showed promise, a lack of willingness and availability to participate among those contacted proved far more problematic. None of the legislators in Florida would agree to participate within the required 90-day timeframe, and so the combination of a lack of legislative data obtained from

Florida's legislative website and a lack of participants resulted in an inability to gather sufficient data on the state of Florida. The researcher requested permission to drop the state and change the study to a single-state case study consisting of California only. The researcher received approval of the committee on December 16th, 2018 and changed the study accordingly.

The researcher removed the data from Florida and performed the data analysis again with only legislation from California. The researcher identified eight legislators who contributed the most to the topics relevant to this study and reached out to their state capitol offices via telephone at the number listed on the California senate web site. Four of the eight declined, three agreed to a written form of the questions, and one agreed to a telephone interview. The researcher then created the questionnaire (Appendix B) and sent it out to all four respondents on November 21, 2018. The researcher conducted the telephone interview on November 29, 2018. The researcher sent out a follow-up email to the three remaining respondents on December 7, 2018 since results had not yet been received by them at that point. One of the respondents declined to participate after reviewing the questionnaire and referred the researcher to a different source. The researcher received one questionnaire response on December 12, 2018. The researcher reached out to the fourth respondent on January 2, 2019 (after the holiday break) and discovered that the individual responsible for coordinating the effort had left the office and hadn't told anyone about the interview. The researcher sent the email thread along with the consent form and questionnaire to the replacement contact on January 2, 2019. The respondent agreed to a telephone interview but stated at the beginning of the interview that they were unable to help but appreciated the interest and would contact the researcher if they could find anyone else that might be able to contribute to the study. This resulted in only two of the original four respondents participating in the survey. This did not provide a sufficient sample size of

participants, and so the survey and interview data were discarded. The discarded data from the study (Instrument development and validation, Data analysis, Survey results, and Implications) are included in Appendix C.

The exclusion of the survey and interview data left only the data collected online, which is not suitable for a case study (Terrell, 2016). However, the data from the California legislative web site proved sufficient to address the research questions in this study on its own. In this case a content analysis is appropriate (Terrell, 2016), and so the researcher changed the study once again. The researcher presented the findings/synthesis of the online data collection. A list of potential participants along with the results of the researcher's attempt to make contact with them is presented in table 1.

Table 1

*List of potential participants and results*

Candidate	State	Result
1	Florida	Unable to make contact
2	Florida	Unable to make contact
3	California	Declined to participate
4	California	Participated via questionnaire (Participant A-2)
5	Florida	Unable to make contact
6	California	Declined to participate
7	Florida	Unable to make contact
8	California	Declined to participate
9	California	Declined to participate
10	California	Participated via telephone interview (Participant A-1)
11	California	Changed their mind. Referred the researcher to C12
12	California	Agreed to telephone interview, then stated they couldn't help
13	Florida	No response to original or follow-up request
14	Florida	No response to original or follow-up request
15	Florida	No response to original or follow-up request
16	Florida	No response to original or follow-up request
17	Florida	Unable to make contact
18	Florida	Unable to make contact
19	California	Staff changes resulted in lost paperwork. Did not participate

This study had the potential to amass a large amount of data, and so it was necessary to define a point at which the study was considered complete. In the case of the literature review, the data was limited to a period of not more than five years and within the scope defined by this study (e-PHI privacy policies best suited to seniors using in-home health monitoring systems). State legislation was broken down into two parts: a review of data available from the state legislative web sites (<http://leginfo.legislature.ca.gov/faces/billSearchClient.xhtml>, <http://leginfo.legislature.ca.gov/faces/legIndexTosaTemplate.xhtml>, and [http://www.legislature.ca.gov/bill\\_index2.html](http://www.legislature.ca.gov/bill_index2.html)) and data obtained from state archives and libraries (when necessary). Obtaining information in this manner could potentially take a significant amount of time, and so data collection terminated after 90 days and included a log of information obtained, by whom, and if data collection was terminated due to no response or inability to access the archival data. This information was included in the analysis section as a caveat to provide clarification and to prevent confusion when data collection was terminated due to no response.

## **Research questions**

The main research question of this work was – what was the California state legislature doing to protect the security and privacy of users of in-home mobile health monitoring systems? Specifically, those developed and maintained by organizations or individuals not classified as covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)?



*RQ 1: What legislation did California have in place governing the development and maintenance of the technology used with mobile in-home health monitoring systems developed and maintained by organizations or individuals not classified as covered entities under HIPAA?*

*RQ2: What legislation did California have in place to protect the privacy of seniors using mobile in-home health monitoring systems developed and maintained by organizations or individuals not classified as covered entities under HIPAA?*

*RQ3: What was the required technical and legal expertise California needed to develop and enforce such legislation?*

### **Specific research method(s) to be employed**

The purpose of this study was to learn what was being done at the legislative level to protect the security and privacy of users using in-home mobile health monitoring systems. Specifically, those developed and maintained by organizations or individuals not classified as covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The study focused on California state legislation using the internet, and so a content analysis was called for.

### **Institutional Review Board (IRB)**

In any study, it is the researcher's responsibility to ensure no physical or psychological harm comes to the participants (Terrell, 2016). The researcher received Institutional Review Board (IRB) approval on November 7, 2017 (See Appendix A for IRB approval).

### **Instrument development and validation**

The researcher collected data via examination of publicly available information. No other instruments were used.

### **Sample**

The researcher examined California, due to its reputation for groundbreaking privacy laws (Lovells, 2013; Willcox, 2017); and high population of seniors (U.S. Census Bureau, 2014). California State legislation was obtained via review of data available from the state legislative web sites (<http://leginfo.legislature.ca.gov/faces/billSearchClient.xhtml>, <http://leginfo.legislature.ca.gov/faces/legIndexTosaTemplate.xhtml>, and [http://www.legislature.ca.gov/bill\\_index2.html](http://www.legislature.ca.gov/bill_index2.html)), and data obtained from state archives and libraries (when necessary).

### **Data analysis**

The researcher conducted a content analysis drawing from Terrell (2016) to conduct data analysis. The researcher conducted a content analysis of California legislation beginning with an extensive review of the literature from the Internet. The researcher analyzed and coded the data to identify patterns, concepts, and relationships.

### **Formats for presenting results**

The results were presented in a tabular format with charts and illustrations as appropriate. Sections were broken down by research question and compared and contrasted the findings of

extant literature and current and proposed legislation. The results of the study are presented in chapter four.

### **Resource requirements**

This study required exhaustive examination of California legislation to learn what was being done at the legislative level to protect the security and privacy of users using in-home mobile health monitoring systems. Specifically, those developed and maintained by organizations or individuals not classified as covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Sources included data available from the Internet and state archives and libraries. A discussion of these resources, as well as additional resources required for data analysis and reporting, follows.

The researcher conducted an exploratory study consisting of a review of state legislation, industry best practices, and extant literature to identify both the current and proposed legislation regarding the protection of e-PHI data of those using in-home health monitoring systems.

### **Summary**

The purpose of this study was to learn what was being done at the legislative level to protect the security and privacy of users using in-home mobile health monitoring systems. Specifically, those developed and maintained by organizations or individuals not classified as covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The researcher conducted a content analysis of California legislation beginning with an extensive review of the literature from the Internet. The researcher analyzed and coded the data

to identify patterns, concepts, and relationships. The results of the study are detailed in chapter four.

## Chapter 4

### Results

#### Introduction

The results of the study are discussed in this chapter. Data were gathered during the period of May 7 to December 12, 2018. The original plan proved inadequate and had to be modified to produce more relevant results. The detailed results are included and discussed. The chapter concludes with a summary of the results.

#### Data Collection

The researcher began with a Boolean search of the literature using terms that best represented the intended direction of the study: *Privacy AND medical*, *Privacy AND medical AND devices*, and *Privacy AND medical AND monitoring*. Although the searches yielded a seemingly large number of hits (Table 2), the search yielded duplicate records and other data not relevant to this study. It became clear that a new search method needed to be used.

Table 2

*Number of hits for California by search term and legislative session*

Search term	2013-2014	2015-2016	2017-2018	Total
Privacy AND Medical	116	113	137	366
Privacy AND Medical AND Devices	33	39	36	108
Privacy AND Medical AND Monitoring	39	48	61	148
Total	188	200	234	622

The researcher further consulted the legislative site for California and found legislative archives listing each bill presented for consideration by topic for each legislative year available.

Using this new method, the researcher was able to gather a much richer pool of data from which to draw that would be broken down by subject. After reviewing all topics/subjects the researcher identified topics relevant to this study as listed in table 3.

Table 3

*Number of bills by topic and year for California*

Topic	Year					Total
	2014	2015	2016	2017	2018	
Aged persons	2	4	2	1	1	10
Computers and technology, Etc.	0	4	3	5	6	18
Data protection authority, California	0	0	0	0	1	1
Identification	1	1	0	0	0	2
Internet	1	3	0	0	1	5
Medi-Cal	0	1	0	0	0	1
Records	2	5	3	1	1	12
Right of privacy	3	0	0	0	1	4
Short titles	1	0	1	0	1	3
Telephone corporations and telephones	1	3	1	0	0	5
Theft	1	0	1	0	0	2
Total	13	22	12	7	13	67

The researcher analyzed and coded the legislation gathered in table 3. Seven themes emerged as a result of the coding process:

- Aging in place,
- Computer crimes,
- Mobile devices and applications,
- Personal information,
- Policies, procedures, and standards,
- Security breach notification, and
- Web site policies.

## Results

Table 4 presents a summary of the results of the data gathered from the legislative search.

Each piece of legislation is listed beneath the research question supported.

Table 4

### *Summary of results*

RQ 1: What legislation did California have in place governing the development and maintenance of the technology used with mobile in-home health monitoring systems developed and maintained by organizations or individuals not classified as covered entities under HIPAA?	
Resource	Subject of bill supporting research question
California A.B. 22 (2017)	Storing and recording electronic media, cloud computing, trusted system. While this legislation does not mention seniors or mobile in-home health monitoring systems specifically, it specifically mentions the technology used with such systems (cloud computing and storing and recording) and establishes a requirement for using a trusted system with regard to protecting data statewide.
California A.B. 32 (2015)	increased protection for computer data and computer systems. This legislation encompasses all users and computer hardware systems - not just seniors and in-home health monitoring systems.
California S.B. 962 (2014)	Requires software solution, hardware solution, or both that can disable the voice communications, text messaging, internet browsing, and mobile software applications. Emergency services and 911 would not be affected.
California A.B. 1681 (2016)	Requires a manufacturer of a smartphone to provide a means of decryption when ordered by the Attorney General or a district attorney.
RQ2: What legislation did California have in place to protect the privacy of seniors using mobile in-home health monitoring systems developed and maintained by organizations or individuals not classified as covered entities under HIPAA?	
California H.R. 10 (2017)	Establishes Data Privacy Day (01/28/2017)
California A.B. 22 (2017)	Storing and recording electronic media, cloud computing, trusted system. While this legislation does not mention seniors or mobile in-home health monitoring systems specifically, it specifically mentions the technology used with such systems (cloud computing and storing and recording) and establishes a requirement for using a trusted system with regard to protecting data statewide.
California A.B. 32 (2015)	increased protection for computer data and computer systems. This legislation encompasses all users and computer hardware systems - not just seniors and in-home health monitoring systems.
California A.B. 83 (2015)	Requires a business to develop and enforce security procedures and practices to protect the information it gathers on California residents. Also requires the business to have a contract with a third party with whom it shares that information to provide the same protection.
California A.B. 259 (2015)	Provides specific details and format for disclosing a breach of personal information. Additionally, requires offer to provide identity theft prevention services for free for a minimum of 12 months.
California A.B. 322 (2015)	Requires social security numbers be encrypted when electronically gathered, stored, or transmitted. Also prohibits use of social security number for web site access unless it was one element of two-factor authentication.
California A.B. 375 (2018)	The California Consumer Privacy Act of 2018. Provides various protections for user's personal information, and guarantees users access to and control over the information.
California A.B. 441 (2015)	identity theft, seniors
California S.B. 570 (2015)	Provides specific details and format for disclosing a breach of personal information.
California S.B. 576 (2015)	Requires a mobile application to tell users when, how, and why their geolocation information is collected, used, and shared. This must be done when the application is installed. The user must provide additional consent before their information is shared.
California A.B. 695 (2015)	A person may not impersonate someone using the internet, a web site, or "other electronic means" when interacting with someone else. This protection covers everyone no matter how they are connected to the internet or what electronic device they are using.
California A.B. 739 (2015)	Requires a person, business, or agency who maintains personal information in electronic format to take appropriate steps to protect the security of the information.
California A.B. 925 (2015)	Prohibits intentional interception or recording communications via cell, cordless, or landline phone without the user's consent.

California S.B. 956 (2016)	Identity theft
California A.B. 964 (2015)	Provides specific details and format for disclosing a breach of personal information.
California S.B. 1026 (2018)	Provides for home modifications for safer living
California S.B. 1121 (2018)	disclosure requirements for businesses that gather personal information
California S.B. 1137 (2016)	Prohibits the introduction, or threat of introduction, of ransomware into a system.
California A.B. 1192 (2015)	Universal privacy policy for mobile platforms. Provides protection to all users of mobile apps, not just seniors using in-home health monitoring systems.
California S.B. 1307 (2014)	Identity theft
California S.B. 1348 (2014)	Data brokers, sale of personal information
California A.B. 1671 (2016)	Protects all users from intentional eavesdropping and recording without consent. Confidential communication with health care provider is specifically mentioned. Also, some components used by in-home health monitoring systems, such as telephones, are included in this legislation and so would provide protection for the system as a whole.
California A.B. 1906 (2018)	This bill addresses security features of Internet-connected devices and requires businesses to protect the personal information it gathers about California residents. All residents are covered, not just seniors.
California A.B. 1950 (2018)	The privacy policy posting, and adherence requirements specified in this legislation provide the user with detailed information on the gathering, sale, and sharing of their information, which allows users to make an informed decision about whether or not they wish to use the service
California A.B. 2167 (2018)	Provides security of data collected by an application interfacing with digital health feedback system.
California A.B. 2182 (2018)	Provides specific details and format for disclosing a breach of personal information.
California A.B. 2306 (2014)	Provides protection from physical and constructive invasion of privacy. Protection applies to all persons regardless of age.
California A.B. 2678 (2018)	Provides specific details and format for disclosing a breach of personal information.
California A.B. 2688 (2016)	requires commercial health monitoring programs provide notice and obtain consent from users before sharing, selling, or disclosing their information.
California A.B. 2828 (2016)	Provides specific details and format for disclosing a breach of personal information, specifically in case where encrypted personal information plus encryption key were definitely or possibly compromised.
RQ3: What was the required technical and legal expertise California needed to develop and enforce such legislation?	

### *Aging in place*

California recognizes that the American population is aging at an increasing rate. On the national level, the federal Centers for Disease Control and Prevention in 2007 found that people age 65 and over represented 12.6 percent of the American population, and that number is expected to climb to 20 percent by 2030 – totaling 70 million, with 12 million residing in California (California A.B. 1261, 2015; California A.C.R. 49, 2015). On the state level, United States Census data reports over four million seniors currently reside in California – making it the largest population in the country (California A.B. 1261, 2015).

Family support is critical in permitting seniors to continue living in their home. However, the physical, emotional, and financial demands on the seniors, loved ones, and society is considerable (California A.C.R. 49, 2015). For example, the California Legislature finds that family caregivers typically spend 20 hours per week providing personal support and managing



the household, and 59% of them are employed either full – or part-time (California A.B. 1744, 2014; California A.C.R. 38, 2015). This contributes approximately 3.9 billion hours and \$47B of value in unpaid services and support, equivalent to 125% of total Medi-Cal spending and 410% of long-term services and support (California A.C.R. 38, 2015). With nearly 75% of seniors living at home and in need of personal assistance relying entirely on unpaid caregivers and 70% of those suffering Alzheimer’s disease and related disorders requiring daily assistance, the impact to California’s health and long-term care service and support infrastructure would be disastrous if family caregivers were no longer in the picture (California A.C.R. 38, 2015).

The California Task Force on Family Caregiving was created to help encourage and empower family caregivers. The task force would consist of 12 members from the research, caregiving, and senior advocacy arenas and would – until July 31, 2018 – consult with current family caregivers, institutional providers, researchers, academics, and resource centers to better understand caregiver challenges and current services available to them. The task force would partner with the California Commission on Aging (whenever possible) and make policy recommendations to the California Legislature (California A.C.R. 38, 2015).

Several efforts have been created over the years to assist in aging. The Dignity at Home and Fall Prevention Program was created to assist seniors in combating injury risks from falls in the home (California S.B. 1026, 2018). Conditions such as narrow doorways, steps, staircases, low electric sockets, and high cabinets can cause difficulties for seniors living alone and increase their risk of falls and injuries. The program provides grants for assessments and modifications of qualified seniors’ homes to provide a safer environment for them to live in. The program also provides for certain equipment and services such as grab bars, hand rails, nonskid surface

treatments, wearable medical alert devices. Eligibility requirements include income, disability, has or is at risk of falling, and is unable to afford the modifications (California S.B. 1026, 2018).

California's commitment to helping seniors live independently dates back to the establishment of Adult Day Health Care (ADHC) in 1974. ADHC centers provide seniors with various health and social services including transportation, meals, assistance with daily activities, and physical and speech therapy. ADHC was an optional benefit of Medi-Cal until the Budget Act of 2011 and the related trailer bill, Chapter 3 of the Statutes of 2011 eliminated it as an option, resulting in a class action lawsuit claiming violation of Americans with Disabilities Act (California A.B. 1261, 2015).

California settled the lawsuit by creating a new program called Community-based Adult Services (CBAS). This program – as April 1, 2012 – replaced ADHC to ensure seniors and individuals with advanced health care needs received the nursing, therapeutic and personal care services, health monitoring, and caregiver support they needed. The program continues to this day (California A.B. 1261, 2015).

### *Computer crimes*

The prevalence of computer technology in society provides a wealth of opportunity for criminals and hackers to gain unauthorized access to computers and data (California A.B. 32, 2015). Seniors and dependent adults may be particularly vulnerable as medications, physical, or mental impairments might make it difficult to protect themselves or identify when they are being taken advantage of. They may also be unable to reliably report criminal conduct or testify in court on their own behalf (California A.B. 1718, 2016; California A.B. 329, 2017). Indeed, California passed legislation requiring the Department of Justice to post a notice on the Attorney

General's web site to warn the public about fraud against seniors and dependent adults, along with guidance on filing a complaint (California A.B. 2721, 2016). Current and proposed California laws provide protection for seniors and dependent adults from false imprisonment (California A.B. 1718, 2016; California A.B. 329, 2017) , and enhanced sentencing for many crimes in cases where victims are seniors (California A.B. 1718, 2016; California A.B. 329, 2017; California A.B. 441, 2015).

The California state legislature recognizes the dangers of computer crimes. Indeed, California A.B. 32 (2015) specifies the following behaviors as a public offense:

- Knowingly accesses and without permission
  - alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.
  - takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
  - adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a public safety infrastructure computer system computer, computer system, or computer network.
  - adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
- Knowingly and without permission
  - uses or causes to be used computer services.
  - disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.
  - provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.
  - accesses or causes to be accessed any computer, computer system, or computer network.
  - uses the Internet domain name or profile of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages or posts and thereby damages or causes damage to a computer, computer data, computer system, or computer network.
  - disrupts or causes the disruption of government computer services or denies or causes the denial of government computer services to an authorized user of a government computer, computer system, or computer network.

- disrupts or causes the disruption of public safety infrastructure computer system computer services or denies or causes the denial of computer services to an authorized user of a public safety infrastructure computer system computer, computer system, or computer network.
- provides or assists in providing a means of accessing a computer, computer system, or public safety infrastructure computer system computer, computer system, or computer network in violation of this section.
- Knowingly introduces any computer contaminant into any
  - computer, computer system, or computer network.
  - public safety infrastructure computer system computer, computer system, or computer network (pp. 3-4).

California provides protection against ransomware as well. A person is punishable whether they personally introduced the ransomware to the system or had someone else do it. Also, any person delivering a letter or other written form threatening or implying is punishable as if the money or ransom were actually obtained (California S.B. 1137, 2016).

Confidential communications are also protected. For example, eavesdropping on or recording a confidential communication conducted over telephone or other device (except a radio) is prohibited by state law (California A.B. 1671, 2016). Communications between two cellular phones, a cell phone and landline, two cordless phones, and a cordless phone and a landline would be protected under proposed legislation (California A.B. 925, 2015). In addition, the contents of a confidential communication with a health care provider may not be shared on social media, internet web sites, or any other forum (California A.B. 1671, 2016).

The Identity Theft Resolution Act requires a debt collector who provided adverse information about a debtor to notify the credit agency that the account is disputed and initiate a review within 10 business days. If the debt collector does not resume collection activities, they must notify the credit agency to delete the adverse information (California A.B. 1723, 2016).

California legislation also provides protection from impersonation. For example, legislation was proposed to provide for civil action against any person who “knowingly and without

consent” impersonates another person via the internet, by web site, or other electronic means and convinces another to believe they are the impersonated person (California A.B. 695, 2015).

Another form of impersonation prohibited in California are the use of bots. California law requires a person who uses a bot to motivate a sale or a vote in an election must provide “clear, conspicuous, and reasonably designed” notice that the person is talking to a bot (California S.B. 1001, 2018).

Identity theft is another problem in society, and California provides protections for that as well. Anyone who uses another person’s identifying information without their consent and uses it to open credit, purchase goods or services, or obtain medical information” is guilty of a crime under California law (California S.B. 1307, 2014; California S.B. 956, 2016). Sale of the stolen information is illegal as well, as is electronic transmission or physical transfer (California S.B. 1307, 2014). For the person whose identity was stolen, however, state law protects the courts to reflect that they were falsely identified as the perpetrator as a result of their identity having been stolen (California S.B. 1307, 2014; California S.B. 956, 2016).

Invasion of privacy is another method of computer crime, and it falls in to two categories: physical invasion of privacy and constructive invasion of privacy. While both types involve an attempt to obtain a visual, audio, or physical image of a person in a way that a “reasonable person” would find offensive, the two differ in terms of method of capture. Physical invasion of privacy requires a physical trespass on a person’s land, whereas constructive invasion of privacy occurs when the desired visual, audio, or physical image is captured using a device designed to be used from a suitable distance so as to make physical trespass unnecessary (California A.B. 2306, 2014).

*Mobile devices and applications*

California introduced legislation requiring a mobile application to provide “clear and conspicuous notice that fully informs consumers when, how, and why their geolocation information will be collected, used, and shared upon installation of the application” (California S.B. 576, 2015) and to obtain additional consent prior to disclosing the information.

The California legislature recognized several years ago the importance of a technological smartphone security solution to protect not only the devices themselves, but of the data they contain (California S.B. 962, 2014). California law now requires smartphones manufactured and sold after July 1, 2015 to contain a software solution, a hardware solution, or both that – when triggered – can disable the voice communications, text messaging, internet browsing, and mobile software applications (not including 911 and emergency services) capabilities of the smartphone when it has been lost or stolen (California S.B. 962, 2014). This solution must be able to withstand a factory reset and prevent anyone other than the authorized user from reactivating the features. The user has the option to disable the feature(s) or opt out at any time. The requirements of the law no longer apply if the smartphone is resold, consigned, or held as collateral (California S.B. 962, 2014).

Proposed California legislation would require a manufacturer or operator of an application that interfaces with a digital health feedback system be equipped with security features to protect the device and the data stored, processed, and transmitted on it from “unauthorized access, destruction, use, modification, or disclosure” (California A.B. 2167, 2018). The same holds true for businesses that gather personal information about California residents (California A.B. 1906, 2018).

Proposed California law considered a business that provides a mobile application that maintains medical information for the purpose of: providing information to the user or health care provider; allowing the user to manage their information; or for the “diagnosis, treatment, or management of a medical condition of the individual” to be a health care provider. It would therefore be subject to the same standards and punishments imposed under law to any other health care provider (California A.B. 2167, 2018).

In addition to protections for smartphones and their operating systems, California law also requires a manufacturer of a smartphone sold or leased in California on or after January 1, 2017 to be able to decrypt the contents of the device when served a court order. If they are unable to do so, a fine of \$2,500 for each instance will be imposed, which they cannot pass on – in whole or in part – to the consumer. Only the Attorney General or a district attorney can enforce the provisions of this law (California A.B. 1681, 2016).

Proposed California law would require the provider of a mobile operating system or platform upon which developers create mobile applications that collect personal data from an individual California user, either through the mobile application or an online service, to create universal privacy policy standards based on transparency, security, and other principles (California A.B. 1192, 2015). The proposed law would also require standards be posted on their web site – in a format accessible to all users – and require the developer to accept them (California A.B. 1192, 2015).

The Confidentiality of Medical Information Act prohibits any business that offers software or hardware to customers – including mobile applications – from “sharing, selling, or otherwise using” a patient’s medical information for any purpose other than that which is required for the patient’s care, unless properly authorized or required by law (California A.B. 2688, 2016).

Additional legislation expanded the protection of user's data to include operators of commercial health monitoring programs. Furthermore, the operator is now required to provide "clear and conspicuous" notice, and to obtain the user's consent before disclosing patient information gathered by the system. Some exemptions to consent were added as well (California A.B. 2688, 2016).

California A.B. 1192 (2015) proposed the following guidance based on the principles of the Fair Information Practices Act for developers and operators of mobile operating systems and platforms:

- Be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personal data.
- Involve individuals in the process of using personal data and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of personal data.
- Specifically articulate the authority that permits the collection of personal data and the purpose or purposes for which the personal data is intended to be used by defining the functional purpose of the mobile application and how an individual's personal data is used to contribute to that functional purpose.
- Only collect personal data that is directly relevant and necessary to accomplish the purpose or purposes for which the personal data is intended to be used, and only retain personal data for as long as necessary to fulfill the specified purpose or purposes.
- Use personal data solely for the purpose or purposes specified in the notice to the user. Sharing personal data should be for a purpose compatible with the purpose or purposes for which the personal data was collected.
- Ensure, to the extent practicable, that personal data is accurate, relevant, timely, and complete.
- Protect personal data in all media through appropriate safeguards against risks, including, but not limited to, loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- Be accountable for complying with the principles of the Fair Information Practices Act, provide training to all employees and contractors who use personal data, and audit the actual use of personal data to demonstrate compliance with the principles of the Fair Information Practices Act and all applicable privacy protection requirements and laws (pp. 3-4).



### *Personal information*

The definition of “Personal information” has evolved considerably over the years (California A.B. 259, 2015; California A.B. 83, 2016; California A.B. 2182, 2018; California S.B. 576, 2015; California A.B. 964, 2015; California S.B. 570, 2015; California A.B. 2828, 2016; California A.B. 2678, 2018; California S.B. 1121, 2018).

For the purposes of this study, the researcher has chosen the definition in California S.B. 1121 (2018) to specify what is meant by personal information. The definition appears below:

“Personal information” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.
- Characteristics of protected classifications under California or federal law.
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Biometric information.
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an Internet Web site, application, or advertisement.
- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
- Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes (pp. 18-19).

California requires a business to develop and enforce security procedures and practices necessary to protect the information it gathers on California residents from unauthorized “access, destruction, use, modification, or disclosure (California A.B. 83, 2016).” Furthermore, the

business must have a contract with a third party with whom it shares information that requires the third party to develop and enforce security procedures and practices necessary to protect the information it gathers on California residents from unauthorized “access, destruction, use, modification, or disclosure (California A.B. 83, 2016).”

Social security number security is also important. Proposed legislation would have made it unlawful for a business to electronically gather, store, or transmit an unencrypted social security number (California A.B. 322, 2015). Nor would a business be allowed to require a person to transmit their social security number over the internet unless: the connection is secure; or the social security number is encrypted (California A.B. 322, 2015). In addition, the social security number could not be used to access a web site unless it was one element of a two-factor authentication solution (California A.B. 322, 2015).

A business must tell consumers what categories of personal information will be collected, why it is being collected, and how it will be used before data collection begins. Furthermore, the business may not collect any other data without expressly notifying the user as above (California S.B. 1121, 2018).

California recognizes that its citizens value their privacy and want more control over their personal information (California A.B. 375, 2018). The California legislation believes that personal information can be better protected by a thorough and continuous examination of the methods by which it is gathered, used, managed, and shared (California H.R. 10, 2017).

Consumers require assurances that there are protections for their personal information, and they have access to and control over it (California A.B. 375, 2018). To that end, the California Consumer Privacy Act of 2018 was enacted. It provides Californians the rights to:

*Know what personal information is being collected about them.*

A consumer can request information from a business that collects personal information about them. Examples include: which types and specific items of information were collected; why the information was collected; and what types of third parties the business shares the information with.

The business must provide the data free of charge and may deliver the data by mail or in electronic format – provided the data does not require any special software to read or transmit (California S.B. 1121, 2018). While a consumer may request this information at any time, the business is only required to provide the data a maximum of twice in any 12-month period (California S.B. 1121, 2018).

*Know whether their personal information is sold or disclosed and to whom.*

A consumer can also request information from a business that sells personal information about them. Examples include: which types of the consumers' personal information the business sold; and the names and types of third parties the business sold the information to, listed by category of information and name of purchaser (California S.B. 1121, 2018).

Once a third party has purchased a consumers' information, they may not sell it to anyone else unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out (California S.B. 1121, 2018; California A.B. 375, 2018).

*Say no to the sale of personal information.*

A business that sells customers' personal information must notify them, and also let them know they have the right to opt out (California S.B. 1121, 2018; California A.B. 375, 2018).

California grants consumers the right to opt out of having their personal information sold. A person has the right to tell a business at any time not to sell their personal information by clicking a link on their homepage named "Do Not Sell My Personal Information." Once clicked,

the link directs the consumer to a page that allows them or an authorized representative to opt out of the sale of their personal information (California S.B. 1121, 2018; California A.B. 375, 2018).

A business must also include an explanation of the consumers' right to opt out in any online privacy policies or California-specific consumer rights disclosure (California S.B. 1121, 2018; California A.B. 375, 2018). Once directed to stop selling personal information, a business must immediately cease selling their information and may not sell any more until specifically authorized by the user (California S.B. 1121, 2018; California A.B. 375, 2018).

California also grants consumers the right to instruct businesses to delete their personal information at any time. Once directed to delete the consumer's personal information, a business must immediately do so and direct any service providers to do the same (California S.B. 1121, 2018). In some cases, a business must retain a consumer's information, such as when it is necessary to (California S.B. 1121, 2018):

- Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.
- Comply with a legal obligation (p. 6).

A business is not required to honor the consumer's request in these cases (California S.B. 1121, 2018).

*Access their personal information.*

California law permits a person to review their personal information that a data broker has collected about them – free of charge – by submitting a request online through a secure system (California S.B. 1348, 2014).

*Equal service and price, even if they exercise their privacy rights.*

A consumer who exercises their privacy rights may not be discriminated against in any way. Some examples of discriminatory behavior include (California S.B. 1121, 2018):

- Denying goods or services.
- Charging a different price, adjusting discounts or benefits, or assessing penalties.
- A different level or quality of goods or services.
- Implying any of the above (p. 9).

Commercial health monitoring programs are also a concern. An operator of a commercial health monitoring program must notify – and obtain consent from – the user before sharing or selling the user’s personally identifiable health information. The request must be separate from any other consent request, specify the name/nature of the third party, and specify the reason for the request. The user must also be notified of the process to withdraw consent (California A.B. 2688, 2016). The user also has the right to review the personally identifiable health information the commercial health monitoring program keeps about them, and to instruct them to delete it. Unlike other entities that are forbidden from assessing charges for providing or deleting customer information, the operator of a commercial health monitoring program may charge a “reasonable administrative” fee for it (California A.B. 2688, 2016).

*Policies, procedures, and standards*

The California Legislature is committed to adopting uniform standards for the purpose of storing and recording public records and other documents electronically and have directed the guidelines and standards set by the American National Standards Institute be adopted statewide (California A.B. 22, 2017; California A.B. 2225, 2018). These standards require the use of a trusted system (California A.B. 22, 2017). According to the California state legislature:

A cloud computing storage service that complies with International Organization for Standardization ISO/IEC 27001:2013, or other applicable industry-recognized standard relating to security techniques and information security management and provides administrative users with controls to prevent stored records from being overwritten, deleted, or altered shall be considered a trusted system (California A.B. 22, 2017, p. 2).

Cloud-based storage and service solutions can provide productive and practical information technology solutions for local government agencies in daily operations and disaster recovery scenarios (California A.B. 2812, 2018). The distributed architecture can help reduce the chances of a single agency losing its data or going dark after a natural disaster (California A.B. 2812, 2018).

There have been additional bills and offices that analyze the current information technology environment and establish procedures and standards for providing protection to critical data systems.

One proposed article of California legislation would have required the office of information security – not later than July 1, 2019 – to review current state agency information security technologies in place to determine if existing policies, procedures, and standards provide sufficient protection in the current information technology security environment (California A.B. 531, 2017). The office would then have been required to develop a plan to implement any

changes it deems necessary to adequately protect the information technology in place (California A.B. 531, 2017).

The California Open Data Standard (California A.B. 1215, 2015) was proposed to accomplish a multitude of tasks. Among the most notable:

1. On or before March 1, 2016, the Chief Data Officer shall prepare and publish a technical standards manual for publishing public data through the Internet Web portal by state agencies for the purpose of making public data available to the greatest number of users and for the greatest number of applications and shall, whenever practicable, use open standards for Internet Web publishing in a machine-readable format.
2. The manual shall identify the policy for each technical standard and specify which types of data the standard applies to, and may recommend or require that public data be published in more than one technical standard. The manual shall include a plan to adopt or utilize an Internet Web application programming interface that permits application programs to request and receive public data directly from the Internet Web portal. The manual and related policies may be updated as necessary (p. 5).

State agencies are always trying to find ways to enhance and improve their transparency, efficiency, and disaster response preparedness (California A.B. 2812, 2018). The Office of Local Cloud Migration and Digital Innovation in the Department of Technology was proposed to assist in these efforts by finding ways to integrate technologies such as cloud-based solutions. The office was also intended to help the agency find ways to be more accessible to the public (California A.B. 2812, 2018).

The California Department of Technology is part of the Government Operations Agency. It is supervised by the Directory of Technology, who is also known as the State Chief Information Officer. Proposed legislation would identify the duties of the Chief Information Officer to include:

- Advising the Governor on the strategic management and direction of the state's information technology resources.
- Establishing and enforcing state information technology strategic plans, policies, standards, and enterprise architecture. The Director of Technology shall consult with the Director of General Services, the Director of Finance, and other relevant agencies

concerning policies and standards these agencies are responsible to issue as they relate to information technology.

- Providing technology direction to agency and department chief information officers to ensure the integration of statewide technology initiatives, compliance with information technology policies and standards, and the promotion of the alignment and effective management of information technology services.
- Establishing performance management and improvement processes to ensure state information technology systems and services are efficient and effective.
- Approving, suspending, terminating, and reinstating information technology projects.
- Developing and tailoring baseline security controls for the state based on emerging industry standards and baseline security controls published by the National Institute of Standards and Technology (NIST). The Director of Technology shall review and revise the state baseline security controls whenever the NIST updates its baseline security controls or advancing industry standards warrant but, in no event, less frequently than once every year. State agencies shall comply with the state baseline security controls and shall not tailor their individual baseline security controls to fall below the state baseline security controls (California A.B. 650, 2017, pp. 2-3).

The California Office of Information Security is a part of the Department of technology. It is supervised by the Chief of the Office of Information Security and is responsible for approving and overseeing information technology projects. California A.B. 670 (2015) states that the Office of Information Security is authorized to:

- perform or direct independent security assessments of any state entity at the expense of the entity being assessed.
- perform or direct information security program audits – at the expense of the entity being audited – to ensure compliance.

Furthermore, California A.B. 670 (2015) states that the Office of Information Security is required to:

- work with the Office of Emergency Services to order – at a minimum – 35 independent security assessments of state entities each year and “determine basic standards of services to be performed as part of an independent security assessment” (California A.B. 670, 2015, p. 3). The results of the assessment are provided to both the Office of Information



Security and the Office of Emergency Services. Because the assessment results contain detailed information about vulnerabilities of critical systems, their release is only authorized to employees and contractors with job-related requirements.

- work with the Office of Emergency Services in ranking state entities according to information security risk.
- report entities that are not compliant with information security requirements to the Department of Technology and the Office of Emergency Services.
- notify the “Office of Emergency Services, Department of the California Highway Patrol, and the Department of Justice of any criminal or alleged criminal cyber activity affecting any state entity or critical infrastructure of state government” (California A.B. 670, 2015, p. 4).

#### *Security breach notification*

California law requires any person, business, or agency who maintains personal information in electronic format to take appropriate steps to protect the security of the information from unauthorized “access, destruction, use, modification, or disclosure” (California A.B. 739, 2016, p. 1). This applies in cases where the data was unencrypted, as well as when it was encrypted, and the encryption key was compromised or believed to be compromised (California A.B. 2828, 2016). The notification must be written in plain language and all information must be listed under specific headings. A sample notification breach form is provided (California S.B. 570, 2015). If an agency was the source of the breach, it must offer to provide identity theft prevention services for free for a minimum of 12 months (California A.B. 259, 2015).

California law requires security breach notice be provided in one of three ways: written, electronic, or substitute notice (California A.B. 2182, 2018; California A.B. 964, 2015; California S.B. 570, 2015; California A.B. 2828, 2016; California A.B. 2678, 2018).

Substitute notice may be used when: it would cost more than \$250,000 to provide notice; if there are more than 500,000 people to be notified; or the agency does not have all the necessary contact information to make the required written or electronic notice. The notice must be delivered: via email notice (if the email addresses are known); and be prominently posted on the agency's Web page (if it has one) for at least 30 days; and major statewide media and the Office of Information Security must be notified (California S.B. 570, 2015; California A.B. 964, 2015; California A.B. 2828, 2016).

California law provides specific requirements for security breach notification, and even provides a sample notification form. Specifically, the format and content of the notification itself must meet the following requirements as specified in California A.B. 2182 (2018):

The notification must:

- Be written in plain language.
- Be titled "Notice of Data Breach."
- Organize the following information under the headings "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information:"
  - The name and contact information of the reporting person or business subject to this section.
  - A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
  - If the information is possible to determine at the time the notice is provided, then any of the following:
    - the date of the breach.
    - the estimated date of the breach, or
    - the date range within which the breach occurred.
  - The notification shall also include the date of the notice.
  - Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

- A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.
- If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.
- Additional information may be provided as a supplement to the notice. Examples include:
  - Information about what the person or business has done to protect individuals whose information has been breached.
  - Advice on steps that the person whose information has been breached may take to protect himself or herself.
- The title and headings must be clearly visible and easily recognizable, and text must use at a minimum 10-point type (pp. 3-5).

An entity is considered compliant with requirements for written notice if they either: use the model security breach notification form in California A.B. 2182 (2018); or they use the headings and information in California A.B. 2182 (2018) previously described here. An entity is considered compliant with requirements for providing electronic notice if they use the headings and information in California A.B. 2182 (2018) previously described above.

If the security breach notification exceeds 500 California residents for a single incident, the person or business must submit an electronic copy of the security breach notification (without personally identifiable information) to the Attorney General (California A.B. 2182, 2018; California A.B. 964, 2015; California S.B. 570, 2015; California A.B. 2828, 2016; California A.B. 2678, 2018).

### *Web site policies*

According to California law, anyone operating a commercial web site or online service that collects personally identifiable information about consumers residing in California who use or visit that site is required to post – and comply with – its privacy policy on that site (California S.B. 1348, 2014; California A.B. 1950, 2018). Those notified of noncompliance have 30 days to post their policy (California A.B. 1950, 2018). Data brokers are subject to law as well, as they must permit an individual to review their personal information and provide them with the option to opt-out of having their information shared or sold. The law requires an opt-out notice be clearly displayed on the web site and contain clear instructions for the user to opt out (California S.B. 1348, 2014). Once received, the data broker must – at no cost to the user – honor the request as expeditiously as possible and may no longer retain any information beyond that which is absolutely necessary to provide the services requested by the user (California S.B. 1348, 2014).

California law sets clear requirements for privacy policies. According to California A.B. 1950 (2018):

The privacy policy ... shall do all of the following:

- Identify the categories of personally identifiable information that the operator collects . . . and the categories of third-party persons or entities with whom the operator may share that personally identifiable information.
- If the operator maintains a process for an individual consumer who uses or visits its commercial Web site or online service to review and request changes to any of his or her personally identifiable information that is collected through the Web site or online service, provide a description of that process.
- Describe the process by which the operator notifies consumers who use or visit its commercial Web site or online service of material changes to the operator's privacy policy for that Web site or online service.
- Identify its effective date.
- Disclose how the operator responds to Web browser "do not track" signals or other mechanisms.
- Disclose whether other parties may collect personally identifiable information.
- Disclose whether the operator utilizes bots for the dissemination of information, and that bots are software that, for purposes of this section, can execute commands, reply

- to messages, gather information, or perform routine tasks such as online searches, either automatically or with minimal human intervention.
- An operator may satisfy the requirement . . . by providing a clear and conspicuous hyperlink in the operator's privacy policy to an online location containing a description, including the effects, of any program or protocol the operator follows that offers the consumer that choice (p. 3).

## Summary

The results of the study are discussed in this chapter. This study was conducted from May 7 to December 12, 2018. A Boolean search of the literature was initially used but proved ineffective due to duplicate records and other irrelevant data. The researcher further consulted the legislative site for California and found legislative archives listing each bill presented for consideration by topic for each legislative year available. Using this new method, the researcher was able to gather a much richer pool of data from which to draw.

The researcher analyzed and coded the legislation gathered. Seven themes emerged as a result of the coding process:

- Aging in place,
- Computer crimes,
- Mobile devices and applications,
- Personal information,
- Policies, procedures, and standards,
- Security breach notification, and
- Web site policies.

### *Aging in place*

California recognizes that the American population is aging at an increasing rate, and that family support is critical in permitting seniors to continue living independent and product lives.

Over the years, efforts such as the California Task Force on Family Caregiving, the Dignity at Home and Fall Prevention Program, and Community-based Adult Services (CBAS) have been put in place to aid seniors and family members both in providing services, support, and care.

### *Computer crimes*

Seniors and dependent adults may be particularly vulnerable to computer crime. In some cases, it may be difficult for someone to adequately identify attempts to take advantage of them or report suspect behavior if medications or impairments are affecting the person's memory or ability to concentrate. The California Attorney General's web site contains a warning notice about the dangers of fraud against seniors and dependent adults and gives guidance filing complaints. Laws have also been passed adding stricter punishment for crimes against seniors. California law addresses other types of computer crime as well. Confidential communications, identity theft, impersonation – both live and via bot, physical and constructive invasion of privacy, and ransomware are all examples of crimes the California legislature has provided protection against for its residents.

### *Mobile devices and applications*

California legislators also recognize the importance of protecting mobile devices and the applications and data they contain. Devices and applications containing such data as geolocation, health, or personal information require protection by various means. Examples include requiring advance disclosure and consent prior to install; the capability to disable features and capabilities if lost or stolen; the ability to decrypt the contents under court order; and protecting against access, change, and deletion from unauthorized users. Protection of user data has also expanded to include commercial health-monitoring systems – requiring clear notice to – and consent from – the user prior to disclosure.

### *Personal information*

“Personal information” is information that either identifies or could be used to identify an individual. California requires a business to notify users of the categories, purpose and use of the personal information it collects prior to collection and may not collect any other data without additional notice and consent. Furthermore, the business is required to have a contract with any third party they share the information with to ensure appropriate security procedures and practices are in place to protect the data as well. The California Consumer Privacy Act of 2018 allows California residents to: know what personal information is being collected about them; know whether their personal information is sold or disclosed and to whom; say no to the sale of personal information; access their personal information; and receive equal service and price, even if they exercise their privacy rights.

### *Policies, procedures, and standards*

The California Office of Information Security is a part of the Department of technology. It is supervised by the Chief of the Office of Information Security and is responsible for approving and overseeing information technology projects. Its duties include ordering independent security assessments of state entities; ranking state entities according to information security risk; and notifying other agencies of confirmed or suspected criminal cyber activity against entities or infrastructure.

### *Security breach notification*

California law requires any person, business, or agency who maintains personal information in electronic format to take appropriate steps to protect the security of the information and to provide proper notification in the case of a breach. California law requires security breach notice be provided in one of three ways: written, electronic, or substitute notice. Substitute notice may

be used when: it would cost more than \$250,000 to provide notice; if there are more than 500,000 people to be notified; or the agency does not have all the necessary contact information to make the required written or electronic notice. If more than 500 California residents are involved in a single incident, an electronic copy of the security breach notification (with PII removed) must be provided to the Attorney General.

#### *Web site policies*

California law requires commercial web site or online service operators that collect PII on California residents to post and comply with its privacy policy. Other legislation ensures that individuals are permitted to review their personal data and opt-it of having it shared or sold. Privacy policy requirements are also clearly established. Examples include: the categories of personally identifiable information collected; the effective date; is the information shared with third parties; and how “do not track” browser commands are handled.



## **Chapter 5**

### **Conclusions, Implications, Recommendations, and Summary**

#### **Introduction**

The goal of this study was to conduct an exploratory study of existing legislation to learn what was being done at the legislative level to protect the security and privacy of users using in-home mobile health monitoring systems. Specifically, those developed and maintained by organizations or individuals not classified as covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This chapter presents the conclusions of this study, and also discusses the implications and limitations of the study, along with recommendations for future studies.

#### **Conclusions**

This work explored existing legislation to learn what was being done at the legislative level to protect the privacy of user data collected, stored, and transmitted by systems or applications developed by entities not covered under existing federal regulations. Specifically, it addressed the risks to seniors relying on in-home health monitoring systems to provide maintenance and early warning of health problems. The literature review revealed that such systems show promise in the home monitoring environment, but they are not without risk. The use of smartphones, home networks, and downloadable apps puts patient privacy at risk (Jiya, 2016), and combining systems that were not initially intended to function together carries additional concerns. Different privacy protection profiles (Calhoun et al., 2012), opt-in/opt-out defaults (Bellman et al., 2001)

and privacy policies that are difficult to read (Burkell & Fortier, 2013b; Bustos-Jiménez, 2014) or are not adhered to by the application (Njie, 2016) also put user data at risk.

The current legislation is complex in both language and scope. Developers may never be fully confident that they are in compliance (Varshney, 2007) due to different interpretations of the regulations, and users may incorrectly assume that a device or app is protected under federal regulations because the FDA labeled it a “medically regulated device” or a “medical app” (Brzan et al., 2016).

Some states have already begun passing legislation to protect patient data at a level beyond what federal regulations require. While some similarities exist, there is no uniformity across states regarding such protection (Health Information & the Law, 2016b).

Three research questions guided this study. Each question is addressed based on the legislation discovered through the five-year search through the state records.

*RQ 1: What legislation did California have in place governing the development and maintenance of the technology used with mobile in-home health monitoring systems developed and maintained by organizations or individuals not classified as covered entities under HIPAA?*

The researcher examined legislation from each of the seven themes identified during the examination of California state legislation:

- Aging in place,
- Computer crimes,
- Mobile devices and applications,
- Personal information,
- Policies, procedures, and standards,
- Security breach notification, and

- Web site policies.

While this examination showed that there is legislative support governing the development of the technology of individual components of the in-home health monitoring systems (e.g., smartphones, wearable medical devices, sensors, recording devices, etc.), it appears that the in-home health monitoring system as a whole is an immature technology and not in wide enough use to warrant legislative attention.

*RQ2: What legislation did California have in place to protect the privacy of seniors using mobile in-home health monitoring systems developed and maintained by organizations or individuals not classified as covered entities under HIPAA?*

Unlike the challenges posed by the development and maintenance of the technology of in-home health monitoring systems, there is actually ample legislation to protect user privacy in mobile in-home health monitoring systems developed and maintained by those not classified as covered entities under HIPAA. California law considers a business or person acting as a covered entity to be a covered entity under certain conditions. In addition, since there is so much privacy law covering the individual components of the system – going so far as to include the user’s domicile – that the privacy of the system itself would not be compromised if deployed as suggested in this study.

*RQ3: What was the required technical and legal expertise California needed to develop and enforce such legislation?*

There is no indication that a state requires any additional expertise – technical or legal – to develop and enforce such legislation. The legislation evaluated over the course of this study demonstrated consistent balance between technical, theoretical, and legal stakeholders.

## **Limitations**

As with any study, this study had limitations. One limitation of this study is that it was a single-case study focusing on California. An analysis of legislation in other states and regions of the United States may yield different perspectives and attitudes, particularly regarding the maturity of in-home health monitoring systems and the appropriateness of regulating them as a whole. Another limitation of this study was the number of participants. Although the interviews yielded rich data, the number of participants was far less than expected. While this may have been a result of the study being conducted during an election year and the subsequent turnover of legislators and staff, future studies would do well to consider the time of year when seeking participants. A third limitation was the time-constraint placed on the data gathering effort of this study. This study had the potential to amass a large amount of data, and so it was necessary to define a point at which the study was considered complete. In the case of the literature review, the data was limited to a period of not more than five years. There are pieces of legislation that were not passed during the time of this study that may be reintroduced in whole or as part of a companion bill and may become law.

## **Implications**

### *Contribution to Literature*

Extant literature recognizes the importance of leveraging mobile technologies as a means of assisting independent living and in-home health monitoring of senior patients (Díaz-Bossini & Moreno, 2014; Reeder et al., 2015), but there are concerns that the protection of patient data might suffer in the interest of technological advancement (Armontrout et al., 2016; Martínez-Pérez et al., 2014). Current federal regulations only cover applications and systems developed for

use by covered entities and their business partners (Paul & Irvine, 2014; Yang & Silverman, 2014), leaving individual states responsible for the protection of individuals using health monitoring apps obtained from open markets. Current literary guidance and regulations concerning privacy of mHealth applications is sparse and confusing, and researchers and clinicians alike are calling for more standardized guidance to enable developers, clinicians, and users to better leverage mHealth technology while preserving privacy and adhering to legal requirements (Armontrout et al., 2016; Health Information & the Law, 2016a; Lewis & Wyatt, 2014). Indeed, there is a call for more work in the area privacy protection for users' data that is collected, stored, and transmitted (Brzan et al., 2016; Martínez-Pérez et al., 2014; Varshney, 2014; Yang & Silverman, 2014).

This study contributes to the body of knowledge in this area by conducting an in-depth review of current and proposed legislation in the state of California for the past five years. The results will help provide future direction for researchers and developers as they struggle to meet the current and future needs of patients using this technology as it matures.

### *Practical Application*

There are practical applications for this study as well. The seven themes identified during this study can serve as a valuable starting point for state legislators to evaluate existing and proposed legislation within the context of medical data to identify the need for legislation to assist in protecting user data against fraud, identity theft, and other damaging consequences that occur because of a data breach.

## **Recommendations**

Three areas of future research were identified. First, this study was limited to a single-case study focusing on California. Future studies would benefit from expanding the study to include other states or geographic regions. Second, only two of the original 14 participants originally identified actually participated in the study. Given the difficulty in identifying and securing participants, future studies might have more success by employing a more general selection criteria for recruiting participants. For example, participants might be more successfully recruited by identifying the committee(s) or subcommittee(s) that are involved in key legislation and contacting the members to elicit their participation as opposed to focusing only on the sponsor of the bill. Lastly, this study was originally designed as a two-state case study consisting of California and Florida but had to be changed to a single-state case study due to a lack of sufficient data from the state legislative website and inability to locate participants from Florida within the specified timeframe. Future studies could stipulate longer data gathering time and produce a study involving multiple states.

## **Summary**

The goal of this study was to conduct an exploratory study of existing legislation to learn what was being done at the legislative level to protect the security and privacy of users using in-home mobile health monitoring systems. Specifically, those developed and maintained by organizations or individuals not classified as covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This chapter presented the conclusions of

this study, and also discussed the implications and limitations of the study, along with recommendations for future studies.

The literature review revealed that such systems show promise in the home monitoring environment, but they are not without risk. The use of smartphones, home networks, and downloadable apps puts patient privacy at risk (Jiya, 2016), and combining systems that were not initially intended to function together carries additional concerns. Different privacy protection profiles (Calhoun et al., 2012), opt-in/opt-out defaults (Bellman et al., 2001) and privacy policies that are difficult to read (Burkell & Fortier, 2013b; Bustos-Jiménez, 2014) or are not adhered to by the application (Njie, 2016) also put user data at risk.

The three research questions were also discussed.

*RQ 1: What legislation did California have in place governing the development and maintenance of the technology used with mobile in-home health monitoring systems developed and maintained by organizations or individuals not classified as covered entities under HIPAA?*

While this examination showed that there is legislative support governing the development of the technology of individual components of the in-home health monitoring systems (e.g., smartphones, wearable medical devices, sensors, recording devices, etc.), it appears that the in-home health monitoring system as a whole is an immature technology and not in wide enough use to warrant legislative attention.

*RQ2: What legislation did California have in place to protect the privacy of seniors using mobile in-home health monitoring systems developed and maintained by organizations or individuals not classified as covered entities under HIPAA?*

Unlike the challenges posed by the development and maintenance of the technology of in-home health monitoring systems, there is actually ample legislation to protect user privacy in

mobile in-home health monitoring systems developed and maintained by those not classified as covered entities under HIPAA. California law considers a business or person acting as a covered entity to be a covered entity under certain conditions. In addition, the volume of privacy law covering the individual components of the system – going so far as to include the user’s domicile – is such that the privacy of the system itself would not be compromised if deployed as suggested in this study.

*RQ3: What was the required technical and legal expertise California needed to develop and enforce such legislation?*

There was no indication that a state required any additional expertise – technical or legal – to develop and enforce such legislation. The legislation evaluated over the course of this study demonstrated consistent balance between technical, theoretical, and legal stakeholders.

This study contributes to the body of knowledge in this area by conducting an in-depth review of current and proposed legislation in the state of California for the past five years. The results will help provide future direction for researchers and developers as they struggle to meet the current and future needs of patients using this technology as it matures. There are practical applications for this study as well. The seven themes identified during this study can serve as a valuable starting point for state legislators to evaluate existing and proposed legislation within the context of medical data to identify the need for legislation to assist in protecting user data against fraud, identity theft, and other damaging consequences that occur because of a data breach.

Three areas of future research were identified. First, expanding the study to include other states or geographic regions. Second, recruiting participants by identifying the committee(s) or subcommittee(s) that are involved in key legislation and contacting the members to elicit their



participation as opposed to focusing only on the sponsor of the bill. Lastly, conducting a multiple-case study by stipulating a longer data gathering time.

The senior population is growing and is expected to exceed 2 billion by the year 2050 (Vuorimaa et al., 2012). Extant literature shows that seniors prefer living at home rather than in a care facility (Vuorimaa et al., 2012), which will place a heavy burden on personal caregivers and family members as current healthcare technology remains mainly limited to hospital, assisted living facilities, and hospice care. As healthcare costs skyrocket and resources become depleted, researchers are calling for the development of a new healthcare model that better addresses these concerns (Dickerson et al., 2011). This work explored existing legislation to learn what was being done at the legislative level to protect the privacy of user data collected, stored, and transmitted by systems or applications developed by entities not covered under existing federal regulations. Specifically, it addressed the risks to seniors relying on in-home health monitoring systems to provide maintenance and early warning of health problems. While this study showed that there is considerable legislative support governing both the development of the technology of individual components and the privacy of those using in-home health monitoring systems, the in-home health monitoring system as a whole is an immature technology and not in wide enough use to warrant specific legislative attention. Furthermore, there is no indication that a state requires any additional expertise – technical or legal – to develop and enforce such legislation. The results of this study can serve as a valuable starting point for state legislators to evaluate existing and proposed legislation within the context of medical data to identify the need for legislation to assist in protecting user data.

## Appendix A

## IRB Approval

**MEMORANDUM**

To: **Robert L Saganich, M.S. IST, B.S. CIS**

From: **Ling Wang, Ph.D.,  
Center Representative, Institutional Review Board**

Date: **November 7, 2017**

Re: **IRB #: 2017-642; Title, “Toward a unified framework of electronic Protected Health Information (e-PHI) privacy protection for seniors – An examination of privacy policy legislation within the United States for in-home health monitoring systems”**

---

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) ( Exempt Category 2)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

- 1) **CONSENT:** If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
- 2) **ADVERSE EVENTS/UNANTICIPATED PROBLEMS:** The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.
- 3) **AMENDMENTS:** Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to

implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Maxine Cohen, Ph.D.  
Ling Wang, Ph.D.

## Appendix B

### Participant Questionnaire

#### **Introduction**

This research will examine the present and proposed state privacy legislation within California to identify those electronic Protected Health Information (e-PHI) privacy policies that are suited to seniors using in-home health monitoring systems. Personal freedom and independence are essential to a person's physical and mental health, and mobile technology applications provide a convenient and economical method for monitoring personal health. Many of these apps are written by third parties, however, which poses serious risks to patient privacy. Current federal regulations only cover applications and systems developed for use by covered entities and their business partners. As a result, the responsibility for protecting the privacy of the individual using health monitoring apps obtained from the open market falls squarely on the states.

This work explores the viability of providing a conceptual framework for states to use when developing legislation to protect the privacy of user data collected, stored, and transmitted by systems or applications developed by entities not covered under existing federal regulations. Specifically, it addresses the risks to seniors relying on in-home health monitoring systems to provide maintenance and early warning of health problems. The legislation made possible by such a framework will enable the enforcement of privacy protections that protect the confidentiality, integrity, and availability of the user's data. Also, the additional measures required by these laws will provide greater protection against fraud, identity theft, and other damaging consequences that occur because of a data breach.

Please consider the following information when answering question 1:

In-home health monitoring systems rely heavily on mobile devices and applications, and a number of bills have been presented that are directed at protecting users from exploitation. Topics of particular interest are: implementing a universal privacy policy for application developers (California A.B. 1192, 2015) ; requiring notification and user consent before gathering/sharing geolocation data (California S.B. 576, 2015) ; requiring commercial health monitoring programs to provide clear notice and obtain user consent before sharing, selling, or disclosing their information (California A.B. 2688, 2016) ; and requiring smartphones and other devices be equipped with security features to prevent unauthorized access and disclosure of information in the case of loss or theft (California A.B. 1906, 2018; California A.B. 2167, 2018).

1. Are you aware of any other legislation (either current or proposed) that might provide the same or similar protection of mobile devices or medical monitoring devices?

Please consider the following information when answering question 2:

Several pieces of legislation expand the definition of “Biometric Information” (California A.B. 83, 2016; California A.B. 375, 2018) to include items that can be used to identify a person’s gait, sleep, or even exercise patterns. This would seem to fit nicely into the arena of in-home health monitoring systems, as they often use such items to determine a change in a person’s behavior and alert to a possible problem.

2. Are you aware of any other legislation (either current or proposed) covering the use of biometric information on mobile devices, specifically apps that collect, store, and transmit protected health information?

Please consider the following information when answering questions 3 and 4:

California remains committed to the protecting the security and independence of seniors (California A.C.R. 38, 2015; California A.C.R. 49, 2015; California S.B. 1026, 2018) are just some examples of the state's commitment to supporting seniors and their families, and to ensure seniors have the resources and protections necessary to remain independent and living in their homes for as long as possible.

In-home health monitoring systems run the gamut from simple wearable devices to hybrid systems capable of interfacing via smartphone or home wi-fi with cameras, microphones, and other sensors placed throughout the home and on/in the body. For the purposes of this study we are focusing only on those systems created by independent third parties not affiliated with medical companies and not classified as covered entities under HIPAA.

3. Are you aware of any other legislation (either current or proposed) governing the development and maintenance of the technology used (e.g., encryption, transmission standards, tamper alarms) of in-home health monitoring systems?
4. Are you aware of any legislation (either current or proposed) governing the privacy of users of mobile in-home health monitoring systems?

Please consider the following information when answering question 5:

Current literary guidance and regulations concerning privacy of mHealth applications is sparse and confusing, and researchers and clinicians alike are calling for more standardized guidance to enable developers, clinicians, and users to better leverage mHealth technology while

preserving privacy and adhering to legal requirements (Armontrout et al., 2016; Health Information & the Law, 2016a; Lewis & Wyatt, 2014).

5. In your opinion, are in-home health monitoring systems as a whole mature enough to warrant legislative attention, or is it better to remain focused on the individual components (e.g., smartphones, wearable monitors, and sensors) until they become more widely used?

This concludes the questions for this study. Thank you so much for your participation!

## Appendix C

### Interview Data

This study had the potential to amass a large amount of data, and so it was necessary to define a point at which the study was considered complete. In the case of the literature review, the data was limited to a period of not more than five years and within the scope defined by this study (e-PHI privacy policies best suited to seniors using in-home health monitoring systems). State legislation was broken down into two parts: a review of data available from the state legislative web sites (<http://leginfo.legislature.ca.gov/faces/billSearchClient.xhtml>, <http://leginfo.legislature.ca.gov/faces/legIndexTosaTemplate.xhtml>, and [http://www.legislature.ca.gov/bill\\_index2.html](http://www.legislature.ca.gov/bill_index2.html)), data obtained from state archives and libraries (when necessary), and interviews with state legislators. Obtaining information in this manner could potentially take a significant amount of time, and so data collection terminated after 90 days and included a log of information obtained, by whom, and if data collection was terminated due to no response or inability to access the archival data. This information was included in the analysis section as a caveat to provide clarification and to prevent confusion when data collection was terminated due to no response.

The researcher conducted personal interviews with members of the state senate and assembly. The researcher ensured the participants were aware that their privacy and security were of utmost concern, and that no information about them or their answers could or would be tied back to them. The researcher also ensured the participants were aware that they had the right to refuse to answer any questions and to terminate the interview at any time without explanation. The



researcher took field notes of the telephone interview that were kept confidential and stored separately along with the written submission.

### **Instrument development and validation**

The researcher identified eight legislators who contributed the most to the topics relevant to this study and reached out to their state capitol offices via telephone at the number listed on the California senate web site. Four of the eight declined, three agreed to a written form of the questions, and one agreed to a telephone interview.

The researcher then created the questionnaire (Appendix B) and sent it out to all four respondents. The questionnaire consisted of five open-ended questions (Appendix B) mapped to the research questions and was designed for use with both written and telephone participants.

The first question was mapped to RQ2 and focused on the extent to which in-home health monitoring systems relied on mobile devices and applications. The participants were presented with some background information for context and asked if they were aware of any current or proposed legislation that might provide that type of protection to medical monitoring systems.

The second question was also mapped to RQ2 and focused on biometric information. The participants were once again presented background information for context and asked if they were aware of any current or proposed legislation covering the use of biometric information on mobile devices, specifically apps that collect, store, and transmit protected health information.

The third question was mapped to RQ1 and focused on the technology of the in-home health monitoring systems themselves. The participants were asked if they were aware of any current or proposed legislation governing the development and maintenance of the technology used in such systems.

The fourth question mapped to RQ1 and focused on the privacy of the user's data on the in-home health monitoring systems. The participants were asked if they were aware of any current or proposed legislation in this area.

The fifth question mapped to RQ3 and focused on in-home health monitoring systems as a whole. The participants were asked their opinion on whether or not in-home health monitoring systems as a whole were mature enough to warrant legislative attention or was it better to remain focused on the individual components.

### **Data analysis**

The researcher conducted a descriptive case study drawing from Terrell (2016) to conduct data analysis. The researcher began with an extensive review of the literature from the Internet, and also conducted interviews with state legislators. The researcher reviewed notes gathered from interviews to ensure accuracy. Once completed, the researcher analyzed and coded data from published sources and interview participants to identify patterns, concepts, and relationships.

### **Survey results**

The survey consisted of five open-ended questions mapped to the research questions being explored in this study (Appendix B). The same format was used for written and telephone participants. The survey and results are described below:

The first question was mapped to RQ2 and focused on the extent to which in-home health monitoring systems relied on mobile devices and applications. The introduction presented four topics of interest and some examples of legislation relevant to each topic. The participant was

then asked if they were aware of any current or proposed legislation that might provide that type of protection to medical monitoring systems. Respondent A-1 was not aware of any such legislation in the works. Respondent A-2 mentioned “technical corrections” to the California Consumer Privacy Act of 2018 but was not aware of any additional legislation in the works.

The second question was also mapped to RQ2 and focused on biometric information. The scenario was given of how aggregated data from multiple sources could identify gait, sleep, or exercise patterns that might help determine a change in a person’s behavior and alert to a possible problem. The participant was then asked if they were aware of any current or proposed legislation covering the use of biometric information on mobile devices, specifically apps that collect, store, and transmit protected health information. Neither respondent A-1 nor A-2 were aware of any such legislation in the works.

The third question was mapped to RQ1 and focused on the technology of the in-home health monitoring systems themselves. The participant was asked if they were aware of any current or proposed legislation governing the development and maintenance of the technology used (e.g., encryption, transmission standards, tamper alarms) of in-home health monitoring systems. Respondent A-1 was not aware of any such legislation in the works. Respondent A-2 was not aware of any such legislation in the works but pointed out that *“existing California law does require reasonable security measures regarding medical information or that pertaining to physical characteristics. Further, this year the Legislature passed SB 327 requiring reasonable security features on connected devices.”*

The fourth question was also mapped to RQ1 and focused on the privacy of the user’s data on the in-home health monitoring systems. The participants were asked if they were aware of any current or proposed legislation governing the privacy of users of mobile in-home health

monitoring systems. Respondent A-1 was not aware of any such legislation in the works.

Respondent A-2 was not aware of any new legislation either but noted *“California law is focuses on the nature of the data and its use, rather than the form of the device that collects or stores the data. Whether one’s personal information is stored on hard copy papers, in the cloud or in the memory of a mobile device shouldn’t impact the requirement of reasonable security measures, transparency of how information is used, the control someone should have to prevent sharing, and accountability for violations of those requirements.”*

The fifth question was mapped to RQ3 and focused on in-home health monitoring systems as a whole. The participants were asked their opinion on whether or not in-home health monitoring systems as a whole were mature enough to warrant legislative attention or was it better to remain focused on the individual components. Respondent A-1 noted that legislating technology usually ends up raising the price and development time of the technology due to the additional requirements. This might end up doing more harm than good, since one of the main advantages of the in-home health monitoring system is that it can be deployed immediately using existing technology at no additional cost. Respondent A-2 acknowledged the concern for privacy such systems introduce and stated that legislation needs to take a proactive approach to consumer protection and information. The respondent notes *“When it comes to regulating the security and privacy of these devices, we need to have a forward-looking approach that’s not limited to existing technologies. The regulatory approach needs to focus on the type of information, whether security measures are appropriate, and who is accessing the information. We can’t afford to wait for emerging technologies to come into the mainstream before we ensure consumers are properly informed and protected”*. The respondent also cited the importance of

implementing and building upon the framework provided by the California Consumer Privacy Act [of 2018].

## **Implications**

### *Practical Application*

The interview and survey feedback provide valuable insight into the possible problems legislators might face when attempting to regulate in-home health monitoring systems as a whole – that of effectively legislating these hybrid systems into a more proprietary solution, which would effectively defeat the purpose of a hybrid system.

## Appendix D

### Informed Consent Form

#### **General Informed Consent Form**

#### **NSU Consent to be in a Research Study Entitled**

*Toward a unified framework of electronic Protected Health Information (e-PHI) privacy protection for seniors – An examination of privacy policy legislation within the United States for in-home health monitoring systems*

#### **Who is doing this research study?**

College: College of Engineering and Computing

Principal Investigator: Saganich, Robert Lee M.S. IST, B.S. CIS

Faculty Advisor/Dissertation Chair: Cohen, Maxine Ph.D.

Co-Investigator(s): None

Site Information: N/A

Funding: Unfunded

#### **What is this study about?**

This is a research study, designed to test and create new ideas that other people can use. The purpose of this research study is to provide a conceptual framework for states to use when developing legislation to protect the privacy of user data that is collected, stored, and transmitted by systems or applications developed by entities that are not covered under existing federal regulations (e.g., HIPAA). Unlike best practices, the legislation made possible by this work will enable the enforcement of privacy protections that protect the confidentiality, integrity, and availability of the user's data. Also, the additional measures required by these laws will provide greater protection against fraud, identity theft, and other damaging consequences that occur because of a data breach.

#### **Why are you asking me to be in this research study?**

You are being asked to be in this research study to obtain clarification of facts or to obtain information about current and proposed privacy legislation not found in the public domain.

This study will include about five people. It is expected that one person will be from this location.

### **What will I be doing if I agree to be in this research study?**

While you are taking part in this research study, there will be one interview of approximately 60 minutes.

Research Study Procedures - as a participant, this is what you will be doing:

This study focuses on state privacy legislation, so we are contacting members of the state privacy office, its equivalent, or state legislators as potential participants. We ask for approximately one hour of your time, depending on your schedule and the amount of information you wish to share.

### **Are there possible risks and discomforts to me?**

This research study involves minimal risk to you. To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life.

- Privacy risks – while we will take precautions to keep your information confidential, there is always a small risk of accidental disclosure. You will not be identified by name, location, or position on the recording or in handwritten notes taken during the interview. However, it is possible that your identity may be deduced based on your voice or references made to your state or office.
- Legal risks – any disclosure that could result in legal risk will be deleted from the interview records. If we are recording, the recording will be deleted and the interview will be restarted.
- Group or community risks – may arise in the event of accidental disclosure as mentioned under Privacy risks and/or Legal risks discussed above.

### **What happens if I do not want to be in this research study?**

You have the right to leave this research study at any time, or not be in it. If you do decide to leave or you decide not to be in the study anymore, you will not get any penalty or lose any services you have a right to get. If you choose to stop being in the study, any information collected about you **before** the date you leave the study will be kept in the research records for 36 months from the conclusion of the study but you may request that it not be used.

### **What if there is new information learned during the study that may affect my decision to remain in the study?**

If significant new information relating to the study becomes available, which may relate to whether you want to remain in this study, this information will be given to you by the investigators. You may be asked to sign a new Informed Consent Form, if the information is given to you after you have joined the study.

**Are there any benefits for taking part in this research study?**

There are no direct benefits from being in this research study. We hope the information learned from this study will aid states in developing legislation to protect the privacy of user data that is collected, stored, and transmitted by systems or applications developed by entities that are not covered under existing federal regulations.

**Will I be paid or be given compensation for being in the study?**

You will not be given any payments or compensation for being in this research study.

**Will it cost me anything?**

There are no costs to you for being in this research study.

**How will you keep my information private?**

Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law and will be limited to people who have a need to review this information. While we will take precautions to keep your information confidential, there is always a small risk of accidental disclosure. You will not be identified, but it is possible that your identity may be deduced based on your position and the state you work in. Our interview(s) will be recorded and transcribed only with your permission. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution, and any regulatory and granting agencies (if applicable). If we publish the results of the study in a scientific journal or book, we will not identify you. All confidential data will be kept securely. Electronic records of our interview(s) will be encrypted, password protected, and stored on a portable drive in a locked cabinet, along with any handwritten notes, emails, or other documentation you provide us. All data will be kept for 36 months and destroyed after that time by a professional shredding service and witnessed by the principal investigator.

**Will there be any Audio or Video Recording?**

With your permission, our interview(s) will be audio recorded and transcribed by the principal investigator. No identifying information (name, location, or position) will be recorded. A random, unique identifier will be generated to identify the interview and will be kept separate from the recording in the locked cabinet mentioned above. This recording will be available to the researcher, the Institutional Review Board and other representatives of this institution, and any regulatory and granting agencies (if applicable). The recording will be retained, stored, and destroyed as stated in the section above.

**Whom can I contact if I have questions, concerns, comments, or complaints?**

If you have questions now, feel free to ask us. If you have more questions about the research, your research rights, or have a research-related injury, please contact:

Primary contact:

Saganich, Robert Lee M.S. IST, B.S. CIS can be reached at 703-216-1872



If primary is not available, contact:  
Cohen, Maxine Ph.D. can be reached at 954- 262- 2072

### **Research Participants Rights**

For questions/concerns regarding your research rights, please contact:

Institutional Review Board  
Nova Southeastern University  
(954) 262-5369 / Toll Free: 1-866-499-0790  
[IRB@nova.edu](mailto:IRB@nova.edu)

You may also visit the NSU IRB website at [www.nova.edu/irb/information-for-research-participants](http://www.nova.edu/irb/information-for-research-participants) for further information regarding your rights as a research participant.

**All space below was intentionally left blank.**

Voluntary Participation - You are not required to participate in this study. In the event you do participate, you may leave this research study at any time. If you leave this research study before it is completed, there will be no penalty to you, and you will not lose any benefits to which you are entitled.

If you agree to participate in this research study, sign this section. You will be given a signed copy of this form to keep. You do not waive any of your legal rights by signing this form.

### **SIGN THIS FORM ONLY IF THE STATEMENTS LISTED BELOW ARE TRUE:**

- You have read the above information.
- Your questions have been answered to your satisfaction about the research.

### **Adult Signature Section**

I have voluntarily decided to take part in this research study.

## Appendix E

### Participant Request Email

From: Robert Saganich <rs1893@mynsu.nova.edu>  
Subject: Interview request for <legislator's title and name>  
Date: <date and time autogenerated by mail client>  
To: <contact at legislator's office>  
Cc: Robert Saganich <rs1893@mynsu.nova.edu>

<Greeting>,

The Capitol office gave me your contact info to send a request for phone interview to <legislator's title and name>. My email to <him or her> is below. I appreciate any assistance you can provide. Thank you very much.

Dear <legislator's title and name>,

My name is Robert Saganich, and I am a doctoral student at Nova Southeastern University in Davie, Fl. I am writing my dissertation on the protection of electronic Protected Health Information gathered and stored on computer systems and mobile devices in California and Florida. Your work has proved invaluable to me in the areas of my research covering: < Select any topics from: aging in place; computer crimes; mobile devices and applications; personal information; policies, procedures, and standards; security breach notification; and web site policies that the legislator has worked on>. I would be grateful for the opportunity to interview you by telephone (preferably within the next two weeks) in support of my research. The interview won't exceed 30 minutes, and I am in Virginia on ET. I would appreciate your insight on the topics I listed above, as well as any policies or security requirements for applications gathering, storing, or forwarding personal identification or protected health information.

I have received Institutional Review Board approval for this study from the university. If you agree to the interview, I will send you an informed consent letter to review and sign beforehand. Dr. Maxine Cohen is my dissertation chair. You can reach her via email at [cohenm@nova.edu](mailto:cohenm@nova.edu) or through the College of Engineering and Computing's website at <https://cec.nova.edu/>. Thank you so much for your time and for considering my request. I hope to hear back from you soon.

Sincerely,  
Robert Saganich  
703-216-1872  
[rs1893@mynsu.nova.edu](mailto:rs1893@mynsu.nova.edu)

## References

- Ackerman, L. (2016). Mobile health and fitness applications and information privacy report to California Consumer Protection Foundation. Retrieved from <https://www.privacyrights.org/mobile-medical-apps-privacy-consumer-report.pdf>
- An act to add and repeal Section 43.99.1 to the Civil Code, relating to civil law., A.B. 739, California Assembly (2016).
- An act to add and repeal Section 9104 to the Welfare and Institutions Code, relating to aging., A.B. 1744, California Assembly (2014).
- An act to add Chapter 5.8 (commencing with Section 11549.30) to Part 1 of Division 3 of Title 2 of the Government Code, relating to open government., A.B. 1215, California Assembly (2015).
- An act to add Chapter 6 (commencing with Section 17940) to Part 3 of Division 7 of the Business and Professions Code, relating to bots., S.B. 1001, California Senate (2018).
- An act to add Chapter 22.3 (commencing with Section 22590) to Division 8 of the Business and Professions Code, relating to personal information., S.B. 1348, California Senate (2014).
- An act to add Chapter 22.4 (commencing with Section 22596) to Division 8 of the Business and Professions Code, relating to privacy., A.B. 2688, California Assembly (2016).
- An act to add Section 1708.87 to the Civil Code, relating to civil law., A.B. 695, California Assembly (2015).
- An act to add Section 22762 to the Business and Professions Code, relating to smartphones., A.B. 1681, California Assembly (2016).
- An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy., A.B. 1906, California Assembly (2018).
- An act to amend Section 368 of the Penal Code, relating to elder abuse., A.B. 1718, California Assembly (2016).

An act to amend Section 368 of the Penal Code, relating to elder and dependent adult abuse., A.B. 329, California Assembly (2017).

An act to amend Section 502 of the Penal Code, relating to computer crimes., A.B. 32, California Assembly (2015).

An act to amend Section 523 of the Penal Code, relating to computer crimes., S.B. 1137, California Senate (2016).

An act to amend Section 1798.29 of the Civil Code, relating to personal information privacy., A.B. 259, California Assembly (2015).

An act to amend Section 1798.81.5 of the Civil Code, relating to personal data., A.B. 83, California Assembly (2016).

An act to amend Section 1798.82 of the Civil Code, relating to privacy., A.B. 2182, California Assembly (2018).

An act to amend Section 12168.7 of the Government Code, relating to state government., A.B. 22, California Assembly (2017).

An act to amend Section 12168.7 of the Government Code, relating to state government., A.B. 2225, California Assembly (2018).

An act to amend Section 22575 of the Business and Professions Code, relating to consumers., A.B. 1950, California Assembly (2018).

An act to amend Section 22577 of, and to add Section 22575.1 to, the Business and Professions Code, relating to privacy., S.B. 576, California Senate (2015).

An act to amend Sections 56.05 and 56.06 of, and to add Chapter 2.6 (commencing with Section 56.18) to Part 2.6 of Division 1 of, the Civil Code, to amend Section 121010 of the Health and Safety Code, and to amend Section 4903.6 of the Labor Code, relating to privacy., A.B. 2167, California Assembly (2018).

An act to amend Sections 632, 633.5, and 637.2 of, and to add Section 632.01 to, the Penal Code, relating to confidential communications., A.B. 1671, California Assembly (2016).

An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to civil law., A.B. 964, California Assembly (2015).

An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to personal information., S.B. 570, California Senate (2015).

An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to personal information., A.B. 2828, California Assembly (2016).

An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to privacy., A.B. 2678, California Assembly (2018).

An act to amend Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155, 1798.185, 1798.192, 1798.196, and 1798.198 of, and to add Section 1798.199 to, the Civil Code, relating to personal information, and declaring the urgency thereof, to take effect immediately., S.B. 1121, California Senate (2018).

Al Ameen, M., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems*, 36(1), 93-101. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/20703745>. doi:10.1007/s10916-010-9449-4

Alcalá, J., Parson, O., & Rogers, A. (2015, 11/04/2015). *Detecting anomalies in activities of daily living of elderly residents via energy disaggregation and Cox processes*. Paper presented at the Proceedings of the 2nd ACM International Conference on Embedded Systems for Energy-Efficient Built Environments.

Ammar, N., Malik, Z., Rezgui, A., & Alodib, M. (2014). MobiDyC: Private mobile-based health data sharing through dynamic context handling. *Procedia Computer Science*, 34, 426-433. Retrieved from <http://www.sciencedirect.com/science/article/pii/S1877050914009041>. doi:<http://dx.doi.org/10.1016/j.procs.2014.07.049>

Armontrout, J., Torous, J., Fisher, M., Drogin, E., & Gutheil, T. (2016). Mobile mental health: Navigating new rules and regulations for digital tools. *Current Psychiatry Reports*, 18(10), 91. Retrieved from <http://dx.doi.org/10.1007/s11920-016-0726-x>. doi:10.1007/s11920-016-0726-x

Assembly Concurrent Resolution No. 38—Relative to unpaid family caregivers., A.C.R. 38, California Assembly (2015).

Avancha, S., Baxi, A., & Kotz, D. (2012). Privacy in mobile technology for personal healthcare. *ACM Computing Surveys*, 45(1), 1-54. Retrieved from <http://dl.acm.org/citation.cfm?id=2379776.2379779>. doi:10.1145/2379776.2379779

Baumer, D., Earp, J. B., & Payton, F. C. (2000). Privacy of medical records. *ACM SIGCAS Computers and Society*, 30(4), 40-47. doi:10.1145/572260.572261

Bellman, S., Johnson, E. J., & Lohse, G. L. (2001). On site: To opt-in or opt-out?: It depends on the question. *Communications of the ACM*, 44(2), 25-27. Retrieved from <http://dl.acm.org/citation.cfm?id=359205.359241>. doi:10.1145/359205.359241

Breaux, T. D., & Anton, A. I. (2008). Analyzing regulatory rules for privacy and security requirements. *IEEE Transactions on Software Engineering*, 34(1), 5-20. Retrieved from <http://dl.acm.org/citation.cfm?id=1340674.1340710>. doi:10.1109/tse.2007.70746

Brzan, P. P., Rotman, E., Pajnikihar, M., & Klanjsek, P. (2016). Mobile applications for control and self management of diabetes: A systematic review. *Journal of Medical Systems*, 40(9), 210. Retrieved from <http://dx.doi.org/10.1007/s10916-016-0564-8>. doi:10.1007/s10916-016-0564-8

Burkell, J., & Fortier, A. (2013a, 11/01/2013). *Privacy policy disclosures of behavioural tracking on consumer health websites*. Paper presented at the Proceedings of the 76th ASIS&T Annual Meeting: Beyond the Cloud: Rethinking Information Boundaries.

Burkell, J., & Fortier, A. (2013b). Privacy policy disclosures of behavioural tracking on consumer health Websites. *Proceedings of the American Society for Information Science and Technology*, 50(1), 1-9. Retrieved from <http://dx.doi.org/10.1002/meet.14505001087>. doi:10.1002/meet.14505001087

Bustos-Jiménez, J. (2014, 09/13/2014). *Do we really need an online informed consent? Discussion from a technocratic point of view*. Paper presented at the Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication.

Caldeira, J. M. L. P., Rodrigues, J. J. P. C., & Lorenz, P. (2012). Toward ubiquitous mobility solutions for body sensor networks on healthcare. *IEEE Communications Magazine*, 50(5), 108-115. doi:10.1109/MCOM.2012.6194390

Calhoun, B. H., Lach, J., Stankovic, J., Wentzloff, D. D., Whitehouse, K., Barth, A. T., . . . Zhang, Y. (2012). Body sensor networks: A holistic approach from silicon to users. *Proceedings of the IEEE*, 100(1), 91-106. doi:10.1109/JPROC.2011.2161240

California Consumer Privacy Act of 2018, The., A.B. 375, California Assembly (2018).

California Senior Bill of Rights., A.C.R. 49, California Assembly (2015).

Choi, Y. B., Capitan, K. E., Krause, J. S., & Streeper, M. M. (2006). Challenges associated with privacy in health care industry: Implementation of HIPAA and the security rules. *J Med Syst*, 30(1), 57-64. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/16548416>. doi:10.1007/s10916-006-7405-0

Cooley Godward, L. L. P. (2016). California Online Privacy Protection Act of 2003. Retrieved from [https://cooley.com/files/ALERT-Cal\\_OPPA.pdf](https://cooley.com/files/ALERT-Cal_OPPA.pdf)

Dhillon, J. S., Ramos, C., Wünsche, B. C., & Lutteroth, C. (2012, 07/02/2012). *Leveraging consumer sensing devices for telehealth*. Paper presented at the Proceedings of the 13th International Conference of the NZ Chapter of the ACM's Special Interest Group on Human-Computer Interaction.

Díaz-Bossini, J.-M., & Moreno, L. (2014). Accessibility to mobile interfaces for older people. *Procedia Computer Science*, 27, 57-66. Retrieved from <http://www.sciencedirect.com/science/article/pii/S1877050914000106>. doi:<http://dx.doi.org/10.1016/j.procs.2014.02.008>

Dickerson, R. F., Gorlin, E. I., & Stankovic, J. A. (2011, 10/10/2011). *Empath: a continuous remote emotional health monitoring system for depressive illness*. Paper presented at the Proceedings of the 2nd ACM Conference on Wireless Health, San Diego, California.

Dignity at Home and Fall Prevention Act, The, S.B. 1026, California Senate (2018).

Fair Information Privacy Act, The, A.B. 1192, California Assembly (2015).

Federal Communications Commission. (2017, 03/08/2017). Wireless Medical Telemetry Service (WMTS). Retrieved from <https://www.fcc.gov/general/wireless-medical-telemetry-service-wmts>

- Ghose, A., Sinha, P., Bhaumik, C., Sinha, A., Agrawal, A., & Dutta Choudhury, A. (2013, 09/08/2013). *UbiHeld: ubiquitous healthcare monitoring system for elderly and chronic patients*. Paper presented at the Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication.
- Hanson, M. A., Powell Jr, H. C., Barth, A. T., Ringgenberg, K., Calhoun, B. H., Aylor, J. H., & Lach, J. (2009). Body area sensor networks: Challenges and opportunities. *Computer*, 42(1), 58-65. doi:10.1109/MC.2009.5
- Health Information & the Law. (2016a). ONC report to Congress: Examining oversight of the privacy & security of health data collected by entities not regulated by HIPAA. Retrieved from <http://www.healthinfo.org/article/onc-report-congress-examining-oversight-privacy-security-health-data-collected-entities-not->
- Health Information & the Law. (2016b). States. Retrieved from <http://www.healthinfo.org/state-landing>
- Jiya, T. (2016). A realisation of ethical concerns with smartphone personal health monitoring apps. *ACM SIGCAS Computers and Society*, 45(3), 313-317. Retrieved from <http://dl.acm.org/citation.cfm?id=2874239.2874285>. doi:10.1145/2874239.2874285
- Lee, S., Kim, Y., Ahn, D., Ha, R., Lee, K., & Cha, H. (2015, 09/07/2015). *Non-obstructive room-level locating system in home environments using activity fingerprints from smartwatch*. Paper presented at the Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing.
- Lewis, T. L., & Wyatt, J. C. (2014). mHealth and mobile medical Apps: A framework to assess risk and promote safer use. *J Med Internet Res*, 16(9), e210. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/25223398>. doi:10.2196/jmir.3133
- Leyva, C. (2013). *HIPAA survival guide for providers: Privacy, security & the HITECH Act Fourth Edition, Omnibus Rule Ready*(4 ed., pp. 75). Retrieved from <http://store.hipaasurvivalguide.com/hipaa-survival-guide-third-edition.html>
- Lovells, H. (2013). California Continues to Shape Privacy and Data Security Standards. Retrieved from <https://iapp.org/news/a/california-continues-to-shape-privacy-and-data-security-standards/>
- Martínez-Pérez, B., de la Torre-Díez, I., & López-Coronado, M. (2014). Privacy and security in mobile health apps: A review and recommendations. *Journal of Medical Systems*, 39(1),



181. Retrieved from <http://dx.doi.org/10.1007/s10916-014-0181-3>. doi:10.1007/s10916-014-0181-3
- Medicare learning network. (2016, 2016, August). HIPAA basics for providers: Privacy, security, and breach notification rules. Retrieved from <https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurity.pdf>
- Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing, NIST SP 800-145*. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
- Njie, C. M. L. (2016). Technical analysis of the data practices and privacy risks of 43 popular mobile health and fitness applications. Retrieved from <https://www.privacyrights.org/mobile-medical-apps-privacy-technologist-research-report.pdf>
- Paul, G., & Irvine, J. (2014, 09/09/2014). *Privacy implications of wearable health devices*. Paper presented at the Proceedings of the 7th ACM International Conference on Security of Information and Networks.
- Reeder, B., Demiris, G., & Thompson, H. J. (2015). Smart Built Environments and Independent Living: A Public Health Perspective. In C. Bodine, S. Helal, T. Gu, & M. Mokhtari (Eds.), *Smart Homes and Health Telematics: 12th International Conference, ICOST 2014, Denver, CO, USA, June 25-27, 2014, Revised Papers* (pp. 219-224). Cham: Springer International Publishing.
- Relative to California Data Privacy Day, H.R. 10, California Assembly (2017).
- Rindfleisch, T. C. (1997). Privacy, information technology, and health care. *Communications of the ACM*, 40(8), 92-100. Retrieved from <http://dl.acm.org/citation.cfm?id=257874.257896>. doi:10.1145/257874.257896
- Rowan, M., & Dehlinger, J. (2014). A privacy policy comparison of health and fitness related mobile applications. *Procedia Computer Science*, 37, 348-355. Retrieved from <http://dx.doi.org/10.1016/j.procs.2014.08.051>. doi:10.1016/j.procs.2014.08.051

- Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., Elmqvist, N., & Diakopoulos, N. (2016). *Designing the User Interface: Strategies for Effective Human-Computer Interaction* (6th ed.): Pearson.
- Shu-Di, B., Yuan-Ting, Z., & Lian-Feng, S. (2005). *Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems*. Paper presented at the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference.
- Sonam, C., & Shubhangini, R. (2014). Ethics in behavioural targeting: Mapping consumers perceptions. *International Journal of Online Marketing (IJOM)*, 4(2), 45-61. Retrieved from <http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/ijom.2014040104>. doi:10.4018/ijom.2014040104
- Sun, J., Fang, Y., & Zhu, X. (2010). Privacy and emergency response in e-healthcare leveraging wireless body sensor networks. *IEEE Wireless Communications*, 17(1), 66-73. doi:10.1109/MWC.2010.5416352
- Terrell, S. R. (2016). *Writing a proposal for your dissertation: Guidelines and examples*: Guilford Publications. Kindle Edition.
- U.S. Census Bureau. (2014, 2014). 65+ in the United States: 2010. Retrieved from <https://www.census.gov/content/dam/Census/library/publications/2014/demo/p23-212.pdf>
- U.S. Department of Health and Human Services. (2003). Summary of the HIPAA Privacy Rule. Retrieved from <https://www.hhs.gov/sites/default/files/privacysummary.pdf>
- U.S. Department of Health and Human Services Food and Drug Administration. (2015). Mobile medical applications: Guidance for industry and Food and Drug Administration staff. Retrieved from <https://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/ucm255978.htm>
- Varshney, U. (2007). Pervasive healthcare and wireless health monitoring. *Mobile Networks & Applications*, 12(2-3), 113-127. Retrieved from <http://search.proquest.com.ezproxylocal.library.nova.edu/docview/36183706?accountid=6579>.

- Varshney, U. (2014). Mobile health: Four emerging themes of research. *Decision Support Systems*, 66, 20-35. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0167923614001754>. doi:<http://dx.doi.org/10.1016/j.dss.2014.06.001>
- Vuorimaa, P., Harmo, P., Hämäläinen, M., Itälä, T., & Miettinen, R. (2012, 06/06/2012). *Active life home: A portal-based home care platform*. Paper presented at the Proceedings of the 5th International Conference on Pervasive Technologies Related to Assistive Environments.
- Wen, J. H., & Tarn, M. J. (2006). Privacy and security in e-healthcare information management. <http://dx.doi.org.ezproxylocal.library.nova.edu/10.1201/1086/43317.10.4.20010901/31772.4>. Retrieved from <http://www.tandfonline.com.ezproxylocal.library.nova.edu/doi/abs/10.1201/1086/43317.10.4.20010901/31772.4>. doi:Information Systems Security, Vol. 10, No. 4, September/October 2001: pp. 1–16
- Willcox, J. K. (2017). States Push Their Own Internet Privacy Rules. Retrieved from <https://www.consumerreports.org/privacy/states-push-their-own-internet-privacy-rules/>
- Yang, Y. T., & Silverman, R. D. (2014). Mobile health applications: The patchwork of legal and liability issues suggests strategies to improve oversight. *Health Affairs*, 33(2), 222-227. Retrieved from <http://search.proquest.com.ezproxylocal.library.nova.edu/docview/1498231581?accountid=6579>.