Summer 2022

Technology Roadmap for Standards of Healthcare Data Cyber Security: Influence of Public Policy on Consumer Healthcare Cyber Security Protections

Alison Nalven
Portland State University

Courtney Wright
Portland State University

Jennifer Lynn Zeitouni
Portland State University

Nolan Thompson
Portland State University

Sara Ferdousi
Portland State University

Technology Roadmap for Standards of Healthcare Data Cyber Security:

Influence of Public Policy on Consumer Healthcare Cybersecurity Protections

Course Title: Engineering Management Synthesis

Course Number: ETM 590

Instructor: Dr. Tugrul Daim

Term: Summer

Year: 2022

Author(s): Alison Nalven, Courtney Wright, Jennifer Lynn Zeitouni, Nolan Thompson, Sara Ferdousi, Saumya Saxena

ETM OFFICE USE ONLY

Report No.:
Type: Student Project
Note:

Table of Contents

I. Abstract

From the dot com boom to now the Internet of Things (IoT) and Machine Learning era, the evolving digital world that people live in has brought new challenges for protecting personal data and information. IoT devices, smart phones, numerous apps, and more constantly collect personal health data with many positive intentions. However, the recent overturning of Roe vs. Wade by the United States Supreme Court has generated concerns in particular on who and how personal health data can be used by both governments and private companies with unintended consequences for users. Cyber security and regulations for protecting personal health data is more important than ever before. Through both a literature review and then the creation of a technology policy based road map, this paper establishes a methodology to answer the following research question:
How will cyber security technology evolve with the influence of public policy in order to better protect consumer healthcare data privacy rights?

II. Introduction

Maintaining cyber security in a continuously evolving digital environment is a challenge for all organizations today and the health care sector is not immune. In 2021, there was a 35% increase in cyber attacks against healthcare systems affecting nearly 45 million people [3]. Organizations managing health data are particularly more vulnerable to cyber attacks due to the critical information possessed by them, which is valuable on the darkweb, be used in ransomware attacks, or otherwise. The need to develop stricter policy standards to protect individuals' healthcare data is more urgent than ever. Another major recent concern is that the digital paper trail from GPS data, texts or period tracking apps could be used to convict women who get abortion services or those who help women obtain those services in states where abortion is now illegal [1, 2, 31]. While the Health Insurance Portability and Accountability Act (HIPAA) was signed into law in 1996 [10], it does not actually protect all patients' health data as it only covers communication between the patient and "covered" entities, such as doctors, hospitals, pharmacies, and insurers[14]. There is a major flaw in HIPAA as it does not protect data on IoT devices or in apps. There is actually no single US law that covers privacy of all types of data and only three states- California, Virginia, and Colorado have comprehensive consumer privacy laws[14]. The world has changed in the past 26 years since the creation of HIPAAand healthcare policy standards need to evolve with the changing times to protect user's health data. As such, this paper will consider the following three areas through research:

1) Privacy of women's health data in the Post-Roe Era

2) Security of medical devices in IoT

3) Privacy of personal health data from insurance companies

The goal of this paper is to create a technology policy road map that outlines the market drivers, technologies, products, policies, and resources necessary to develop improved standards to safeguard critical healthcare data.

III. Methodology

The team adapted a technology roadmap format to help define the issues with cybersecurity policies, along with providing standards that can be used to create policy. The start to the roadmap is the literature review. Next, the team used the gathered information to create a set of market segments to be used, as well as a driver mind map. The drivers were then measured against the market segments in a table, ranking each driver against each market segment with a value of 1, 2, or 4, to determine which drivers were the most important in this roadmap. This creates a driver vs. market segment QFD. After the drivers were ranked, project features were identified using a combination of the literature review and driver rankings. Once these features were fully defined in a mind map, another QFD was generated to determine the value of each product feature. This was done by measuring the features vs. the drivers. Up until this point, this is a fairly normal process of generating a technology roadmap. However, the goal of the team was to create a health data and cyber security protection standards roadmap. In addition to researching specific emerging technologies that can help create the desired product features, the team researched policy in order to better understand what policies are currently in place and what policies would be needed to fulfill the goals of the product features. This approach to understanding policy's interaction with technology in emerging markets was employed in another body of research on the growth of wind energy industry in China [36]. From the policy research, gaps were then identified, along with a policy mind map to define specific policies to be used. These policies were then measured against product features in another QFD to determine the most valuable policies. Afterwards the team had enough information to create the final roadmap. All of these steps were done collaboratively by the team, discussing and working together to create QFDs and mind maps that were well defined and thought out. The final step was to link all the aspects together in the technology road map, providing information on the Drivers, Product Features, Technology (Policies) and Resources available, and how they relate to each other. Conclusions are drawn by using this roadmap to determine which policies are most important for the team to create an effective set of standards for cyber security around personal data in healthcare.

IV. Literature Review

In today's digital world, cybersecurity in healthcare plays a pivotal role in the organization's processes and functions. As the technology progresses, so do the threats and crimes associated with it. Many articles and papers were reviewed for this project to understand the challenges faced in healthcare cybersecurity and what type of policies can be used to address these

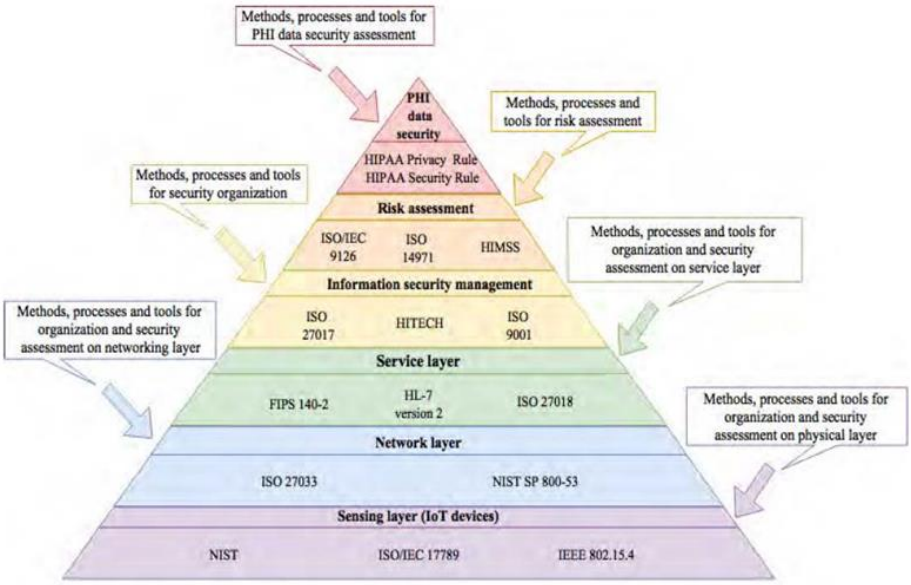
challenges. The most significant papers found in the conducted research have been briefly discussed below:

Cybersecurity of Healthcare IoT-Based Systems: Regulation and Case-Oriented Assessment, 2018

This paper discusses the exponentially growing – IOT (Internet of Things Technology) in the field of healthcare and proposes a normative hierarchical model of the international cybersecurity standards. The authors have identified four major issues in networked healthcare and medical devices – random failures, privacy, deliberate disruption, and malware disruption. These issues and the fact that international regulations and standards do not include any formal technique for cybersecurity assessment of IoT healthcare solutions, make the implementation of the assessment process one-sided and complicated. That is why the authors have developed an approach that considers multiple aspects of development, regulations, standards, security, risks etc.

The healthcare system is divided into seven layers and for each layer the standards and regulations required for security are added resulting in the following hierarchical model [28].

Figure1 :



Proposed Hierarchical Model

Yet Another Cybersecurity Roadmapping Methodology, 2015

This paper describes roadmapping methodology to develop a research roadmap for cybercrime and cyber terrorism. It addresses the fact that cybercrime and cyber terrorism co-evolve with their environment and thus makes the roadmapping task challenging. The authors have developed a four-step methodology based on scenario analysis techniques [29].

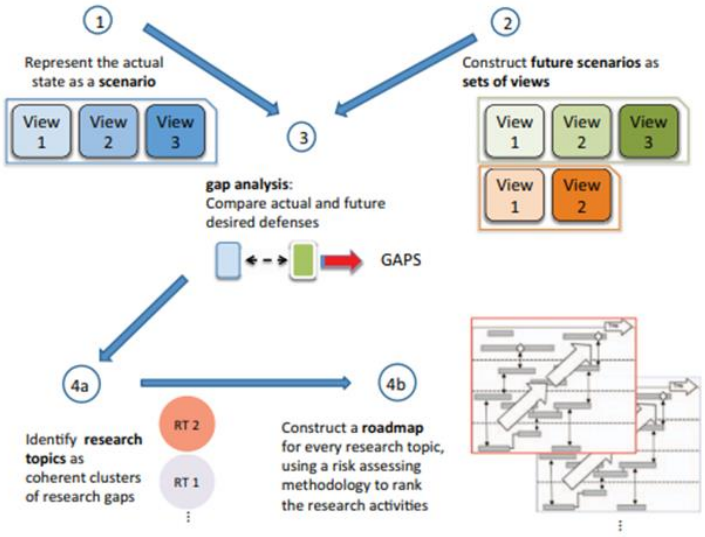


Figure 2: Proposed Methodology

Step 1: Actual State Scenario

The actual state is described as a scenario and consists of a short summary of the contextual environment, followed by the existing cybercrimes and cyber threats along with the available defenses.

Step 2: Scenario Building

The goal of this step is to produce a set of possible future scenarios, which should explore a range of potential evolutions of cybercrimes and cyber threats and of their contextual environment as wide as possible. The step highlights the threats that can emerge, and the corresponding, desirable defenses.

Step 3: Gap Analysis

This step identifies the research gaps that arise from the comparison of each of the future views against the actual state views. Research gaps are identified by tracking the changes of the threats from the actual to the future scenarios and comparing the corresponding existing and desired defenses.

Step 4: Roadmap Construction

The roadmap addressing the research gaps is built as follows:

- Define a set of broad research topics that are related and can be addressed by suitable research actions
- Prioritize the research topics using an appropriate risk assessment method.

- Define a vertical roadmap for each identified research topic. This includes first identifying the research actions required to address the identified gaps, and then describing the actions in a clear time frame, by considering their interdependencies.

Internet of Things realizing the potential of a trusted smart world, 2018

This report examines the policy changes for IoT and lists issues to be considered for effective policy. It has divided IoT applications into three broad categories - Industrial, Public Space and Consumer. It highlights that policies and technologies become more effective if based on the understanding of interdependent social and technical factors. The paper evaluates the following four major frameworks which apply to aspects of IoT. The paper describes that these frameworks have been developed separately and need to be aligned with each other in their development stages [30].

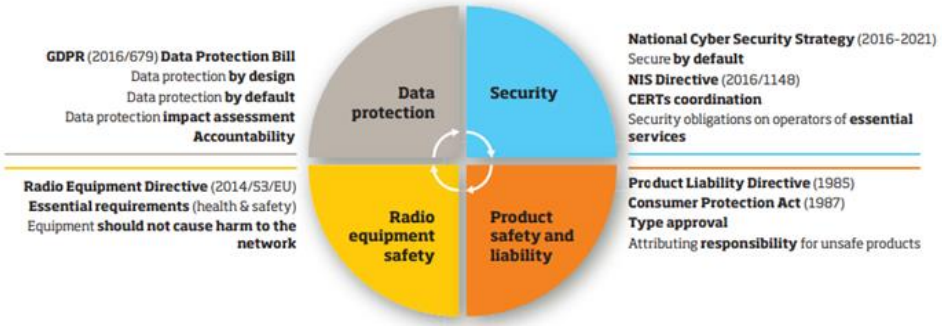


Figure 3: Main regulatory frameworks which apply to IoT

V.Results

Market Segments

As part of this project, the team performed individual research on the topic and identified the market segments. Primary markets deduced through literature review and brainstorming sessions are: Healthcare Institutions, Technology Industry, Consumers and Government.

Healthcare Institutions:

Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a HIPAA covered entity [18]. Health care providers

include all “providers of services” (e.g., institutional providers such as hospitals) and “providers of medical or health services” (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care [18]. Policies on healthcare data protection have a major impact on these institutions. While being HIPAA covered entities they must comply with the Rules requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information [18], any new laws or policies will affect them too. They are often the data originators and other entities can access data through them. Once data leaves their control, healthcare providers may or may not be held responsible for the privacy and security of that information.

Technology Industry:

Big technology companies such as Google, Amazon and Facebook are all looking for an entry into the healthcare market [19]. There are financial interests and vast sums of money to be made based on health records. Lobbying efforts by Silicon Valley encouraged the Department of Health and Human services to draft The Cures Act, which will facilitate data sharing with software companies [20]. This in turn will potentially allow Amazon, Google and Microsoft a dominant position in the service-based cloud storage of health records. Health data collected by wearable devices and apps such as Fitbit and Apple Watch are not protected by HIPAA [20,14]. Latest Apple Watches can take echocardiograms and detect falls but the data set created and communication systems for transferring this data make it hard to protect privacy [20]. Health researchers predict a future with smart homes, which feature technologies like mirrors that detect skin and heart conditions, and mattresses that check vital signs may not be subject to HIPAA regulation if the companies developing the devices are outside the healthcare system [21].

Consumers:

Consumers include patients and anyone who uses healthcare applications including mental health apps, Flo and wearables such as Fitbit, Apple watch or any health monitoring device as well as anyone who purchases healthcare products over the internet. Health data protection policies should be created based on consumers interest. In many cases consumers are not savvy enough to understand that their personal data can be sold once it’s outside the healthcare system [22] or how many times the data they input through health applications are sold to multiple parties. As a ramification of Roe v. Wade overturned by the supreme court, female health information may be used to criminalize consumers. Millions of digital traces from social media accounts and devices

that are plugged into algorithms to predict health outcomes, these may be expanded from data mining and could be used for consumer profiling or marketing purposes [21].

Government:

This segment includes both federal, Congress, Department of Health and Human Services Federal Trade Commission, and state level government. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), a federal law, was enacted on August 21, 1996 [18]. However not all health related information falls under its purview [20,14]. Due to the lack of comprehensive federal privacy laws regulating health technology companies, some states enacted their own data privacy laws. Currently, three states: California, Colorado and Virginia have comprehensive consumer privacy laws. Four other states, Massachusetts, New York, North Carolina, and Pennsylvania, have serious comprehensive consumer data privacy proposals in committee [14].

Market Drivers

Technology:

Advancement in technology and its omnipresence in current daily life is a major driver for data privacy policies. The rapid pace of health application development and the bureaucratic delay of policy enactment has created a gray area where tech companies can collect, store and share consumer health data without being accountable. The Federal Trade Commission (FTC) utilizes existing statutory authorities and its power to ensure apps are keeping their promises to consumers around the handling of their sensitive health information, however, there is a need for comprehensive federal privacy legislation to regulate personal health information collected by latest technologies. Such legislation will encourage security measures around health apps and provide consumers of such technologies to be aware of how their PHI is being handled.

Safety:

Personal health information data breach can cause direct harm to a patient or a consumer of health apps. Cyberattacks on electronic health records and other systems also pose a risk to patient privacy because hackers access to PHI and other sensitive information [26]. Particularly, women's fertility health information could be used against them in the states where abortion is banned. HIPAA has provisions for sharing health data safely for research purposes, however, data collected by various apps are not covered by those. In 2021, Flo Health took control of users' sensitive fertility data and shared it with third parties despite expressing privacy claims. This left consumers feeling outraged, victimized and violated [27]. Incidents as such calls for

more policies around data safety and privacy. In turn the tech companies will adopt and change their behavior around consumer PHI.

Social & Economic:

In the age of "surveillance capitalism", data collected through nonstop interactions with digital technologies are being commodified and traded. New digital health technologies and increased awareness about public health due to the COVID-19 pandemic may pave the way for a fundamental shift in healthcare data privacy [21]. Rise in the demand for virtual care enabled technology companies to proliferate the healthcare market. This in turn made healthcare a lucrative field. Soaring healthcare costs contributed towards the reliance on healthcare applications. Seemingly free health applications are often making profit through trading in private data of the users. This seismic shift in society's view on data privacy is a major driver for public policies on protecting personal health information.

Government:

Government plays the most important role in creating public policies to regulate how companies handle consumer data. Congress enacted Health Insurance Portability and Accountability Act ("HIPAA") in 1996 to protect health data [18]. Federal Trade Commision (FTC)'s Health Breach Notification Rule ensures that entities who are not covered by HIPAA face accountability when consumers' sensitive health information is compromised [23].

Figure 4 : Market Drivers Mind Map

Market Segments Vs. Drivers Mind Map and QFD

The QFD is an imperative part of the technology roadmapping process. With the drivers and segments defined, the team was able to move forward with the comparisons. The mind map for the drivers is shown above:

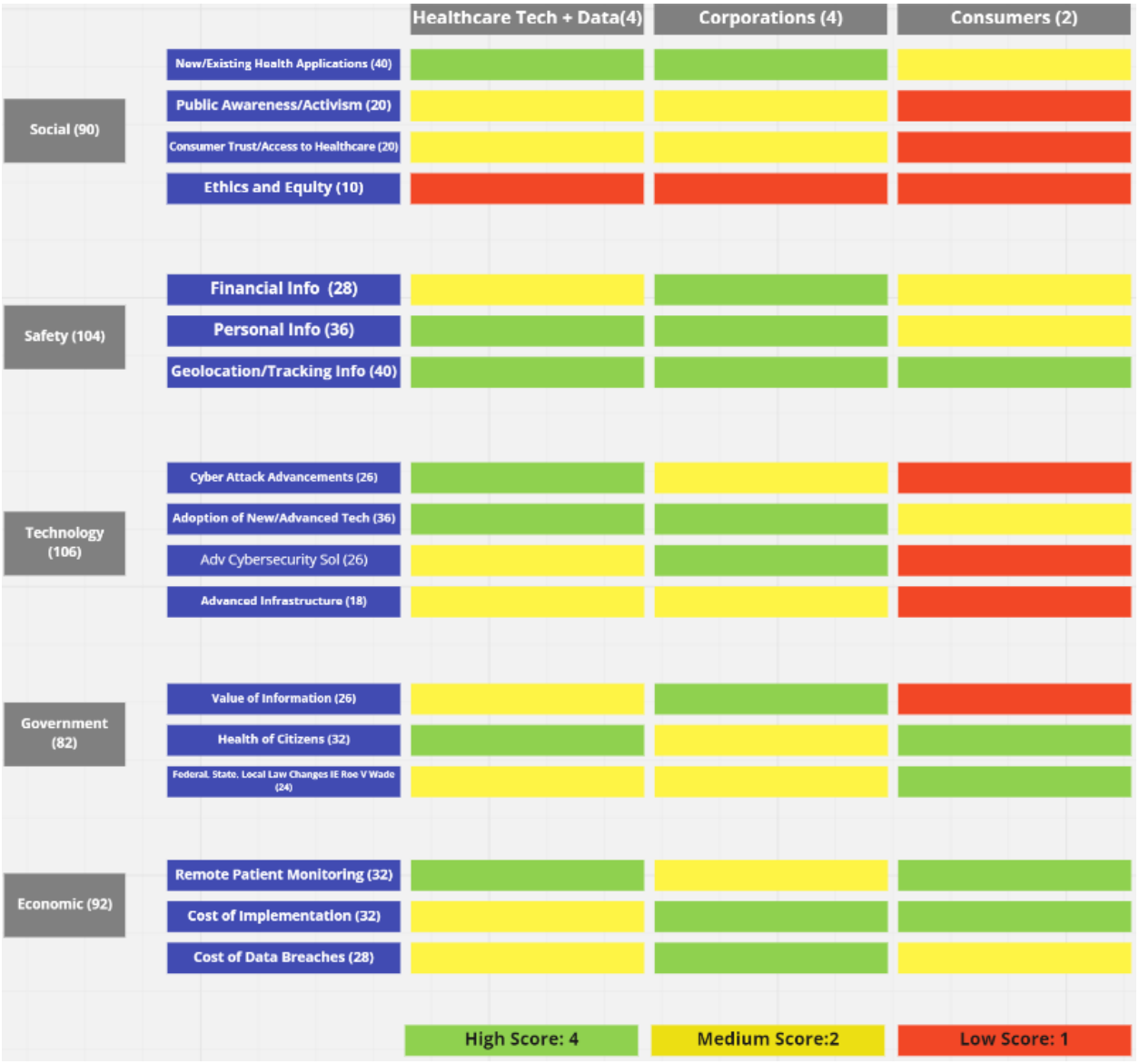


Figure 5 : Market Segments v. Drivers QFD

Each section of drivers has multiple specific portions that were measured against each of the market segments to create the QFD. When considering what the safety driver was, the team specifically thought of data safety. Is it safe from those who wish to use it maliciously? Is it appropriately stored? Are there laws defining how the data can be used or sold? All of these thoughts come from the safety driver. The team used this to guide the choices in the QFD. When considering personal info in regards to healthcare + data and corporation segments were rated highly, along with geolocation/tracking info along all segments. Consumers of the data don't really care how they use their own information, they want it stored appropriately, but it's much more important how corporations use it when it is given. This is the thought process the team used to rank all the drivers vs. the segments in the QFD, shown above.

Market Drivers VS. Product Features Mind Map & QFD

After the team ranked the drivers, creating a product features mind map, then comparing the drivers vs. the product features was the next step. The sets of product features the team produced were Dynamic change, meaning the standards can update as technology and needs advance. Data protection, specifying exactly how data can be used, stored, and required levels of protection from malicious attacks. Effective Federal Policy, meaning it creates a baseline that all states must adhere to, which covers all individuals. Data Breach Response, which defines what the company is required to do when a data breach occurs. Looking at timeline for a fix, timeline for updated security measures, and restitution requirements for value of data lost. Finally Inform Consumers looks at how a company must let a consumer know what their data is being used for, along with the protections they have in place for said data. The mind map and QFD are found on this page.

Figure 6: Market Drivers v. Product Features Mind Map

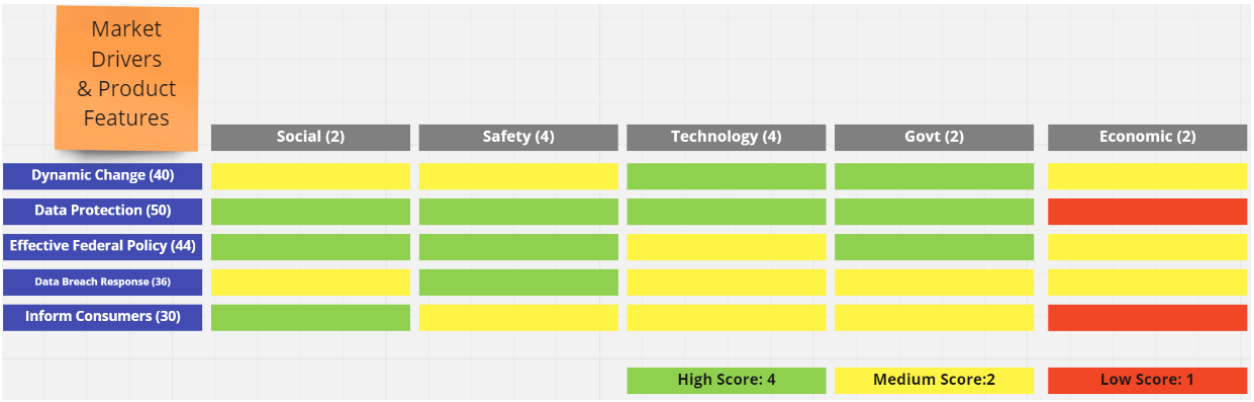


Figure 7 : Market Drivers v. Product Features QFD

Policy Mind Map

Much of the technology exists to adequately protect consumer data privacy. Public policy will be the key catalyst to expedite the implementation of cybersecurity technology by corporations. Public officials and non-profit organizations such as the ACLU have proposed policies to advance consumer data privacy, which were reviewed in this research - as displayed in the figure below.

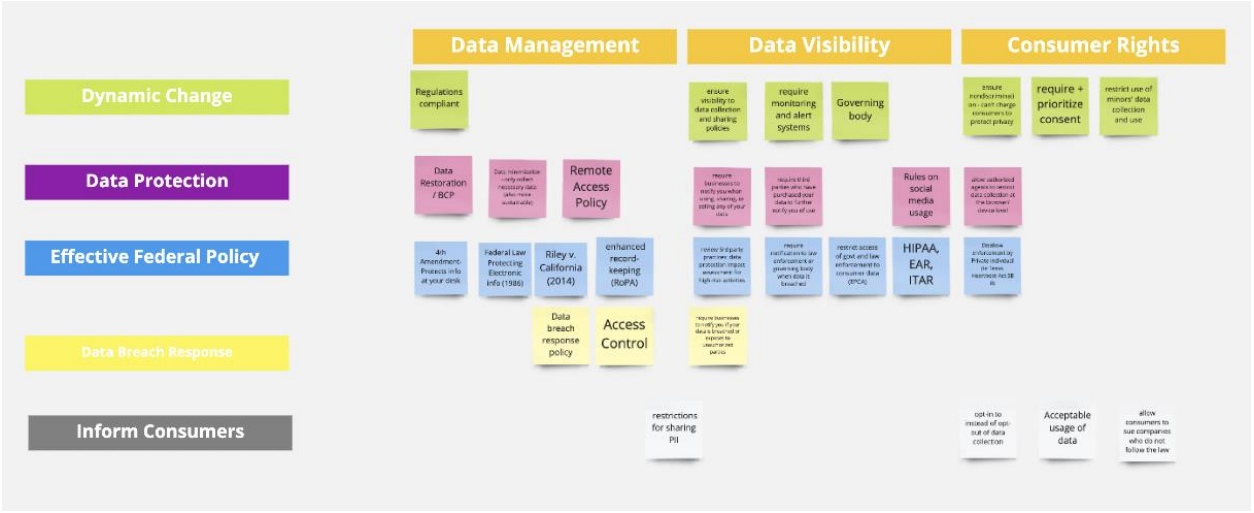


Figure 8 : Policy Mind Map

Consumer data privacy public policy was categorized into three main themes: data management, data visibility, and consumer rights. The policy points were then mapped to align with the previously discussed product features. Data management policy will ensure that technology remains compliant with the dynamic regulations, minimize data collection to only necessary information, expand 4th amendment rights and enhance record keeping capabilities, as well as enforce data breach response policy. Data visibility policy will ensure corporations provide a means for consumers and governing bodies to review data collection, storage, and sharing policies, institute an external governing body to ensure compliance, require companies to

complete risk assessments when sharing data with partners, and restrict access to consumer data by government agencies and law enforcement. Consumer rights policy will ensure nondiscrimination so that consumers won't have to pay to maintain their privacy, require and prioritize consent by allowing authorized agents, such as web browser filters, to restrict data collection at the browser and device level, reduce the burden on consumers by requiring opt-in instead of opt-out consent, and restrict the use of minors' data. [16, 17]

Product & Technology Features QFD

To determine the priority of the technology policy features identified, a QFD was conducted in consideration of the desired product features. The product feature weights were based on those determined with the Market Driver & Product Feature QFD outlined above. Data visibility policy was determined to be the most important technology feature, as it significantly impacts data protection, effective federal policy, data breach response, and informing consumers. Consumer rights policy was the second most important technology feature, as it significantly influences data protection and informing consumers. While data management has a significant impact on data breach response, it was determined to be the least important as it has just a medium impact on other product features. These findings are all outlined in the figure below.

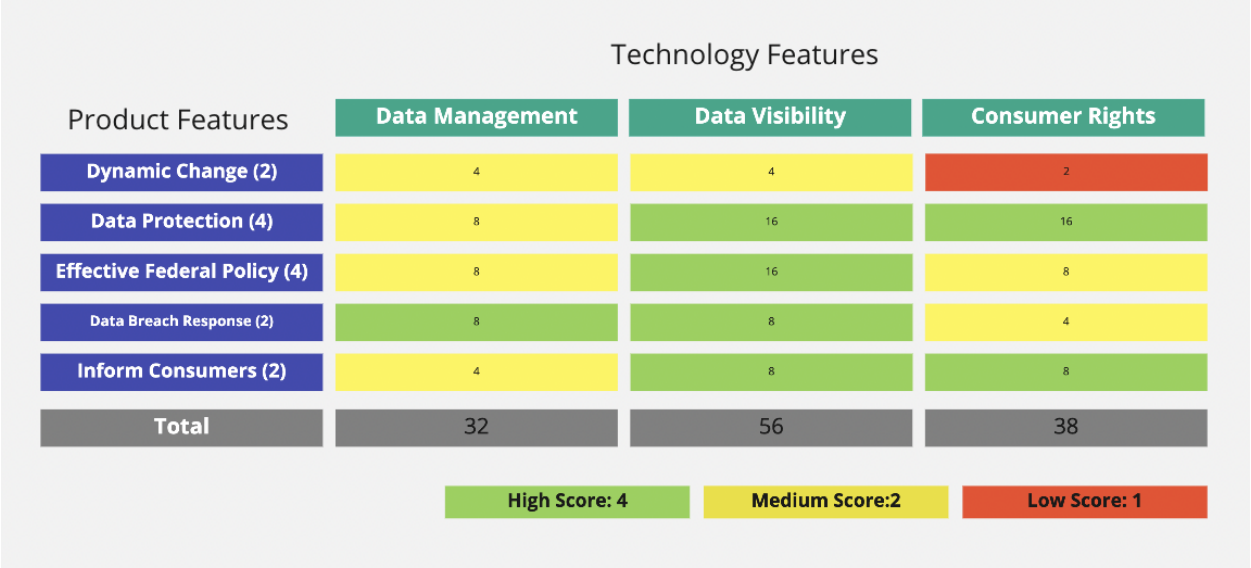


Figure 9: Technology Policy v. Product Features QFD

GAP Analysis

Data Protection:

HIPAA rules protect the privacy and security of certain health information and require certain entities to provide notifications of health information breaches [14]. A recent policy statement on this Rule considers apps covered by the Rule if they are capable of drawing information from multiple sources, such as through a combination of consumer inputs and application programming interfaces [25]. However, this does not extend to the smartphone apps that collect information through user input [14]. There is a need for a national framework to protect consumer data privacy, give consumers protections against the discriminatory use of their data, and mandate that companies minimize the amount of data they need to collect to deliver products and services [25, 27].

Federal Policies:

In recent times, very little has been done to protect and secure personal health information (PHI). There is a patchwork of legislation currently existing to protect different types of private data such as FCRA for credit records, FERPA for student records and HIPAA for personal health information. HIPAA's disclosure rules, which took effect in 2003, don't apply to personal health data in general, just the patient information flowing through the health-care system [25]. Legislators have been trying to enact a comprehensive national privacy standard for ages and only recently congressional leaders released a bipartisan draft bill called the American Data Privacy and Protection Act (ADPPA) [25]. There are also a handful of state laws on consumer privacy protection and these current assortment of laws lead to unnecessary confusion and complexity [25].

Dynamic Change:

Healthcare technology is advancing at an unprecedented scale. Since the Covid-19 Pandemic the usage of healthcare applications has increased multiple fold. Research from the Organization for the Review of Care and Health Applications found that the COVID-19 pandemic led to a twenty five percent increase in health app downloads, and that, of the 350,000 health apps available on the market, 90,000 were introduced in 2020 alone, an average of 250 per day [24]. While there is a clear need to modernize the healthcare system, the complexity of the undertaking has made a tough go due to consumer personal information privacy and security fear [20]. The Cures Act drafted by the Department of Health and Human Services includes provisions to share electronic health information but it does not contain any rules on data privacy [20, 22]. This rule will ease the way for big tech companies to mine personal health information from HIPAA covered

organizations. But once the information is out of a HIPAA covered entity's control, the question of data security and protection responsibility remains unanswered [22].

Inform Consumers:

Looking closer at Inform Consumers the team thinks HIPAA, or a similar policy should be expanded to cover personal health data that may not currently be covered. An example of this is period tracking apps, and other information related to reproductive health. In addition to the HIPAA rules, it's important that if a company collects consumer data, it clearly states the data is being collected before the collection starts. Additionally, the reason for collecting the data needs to be stated. The purpose of data collection could include use to feed an algorithm and improve the application, sale to profit the corporation, or use to benefit the consumer in one way or another. Whatever the use of data may be, the consumer needs to be informed prior to the collection and use of said data. This is an imperative step in educating consumers on how valuable their data may be, while helping them to further protect themselves from malicious entities who might want to use that data inappropriately. An additional objective for the phase II requirement of informing consumers would be to require that the healthcare covered entity document a mandatory recurring training to all involved personnel, as well as the content of the HIPAA enforcement rule showcasing the penalties of HIPAA violations. In order to have better informed consumers, authorization and consent forms must be mandatory in all covered entities, and consumers must know the process to follow in case of any HIPAA violations.

Data Breach Response:

Data breach response, as discussed earlier, is what a company does when valuable personal data they are storing is released unintentionally to others. An example of an effective and meaningful response was the $5 billion penalty imposed on Facebook by the FTC in 2019 for violating a 2012 order by deceiving users about Personal Identifiable Information (PII) privacy. This was approximately 20 times greater than any data privacy or cybersecurity penalty imposed globally. [35] While this response to Facebook's deceptive policies was historically bold, the only current comprehensive federal requirement is that corporations notify affected parties and government agencies about a data breach. While there are many state policies that can impose fines for failing to notify, along with allowing for civil suits, there are no clear ways for the victims of these breaches to regain anything of value from what was lost. The team recommends a federal baseline of restitution for data lost, the value of which can be defined by research within government agencies, and a timeline for when the organization will understand why the breach happened and what they are doing to fix it. Additionally, there needs to be increased or improved monitoring of collected and stored data to understand if a data breach has happened, or if it is currently happening in order to reduce the amount of damage that occurs from the data breach.

Technology Roadmap

Based on previous information, the roadmap below, which consists of four main sections, was created. These sections as well as the legend for the roadmap are developed in the following paragraphs.

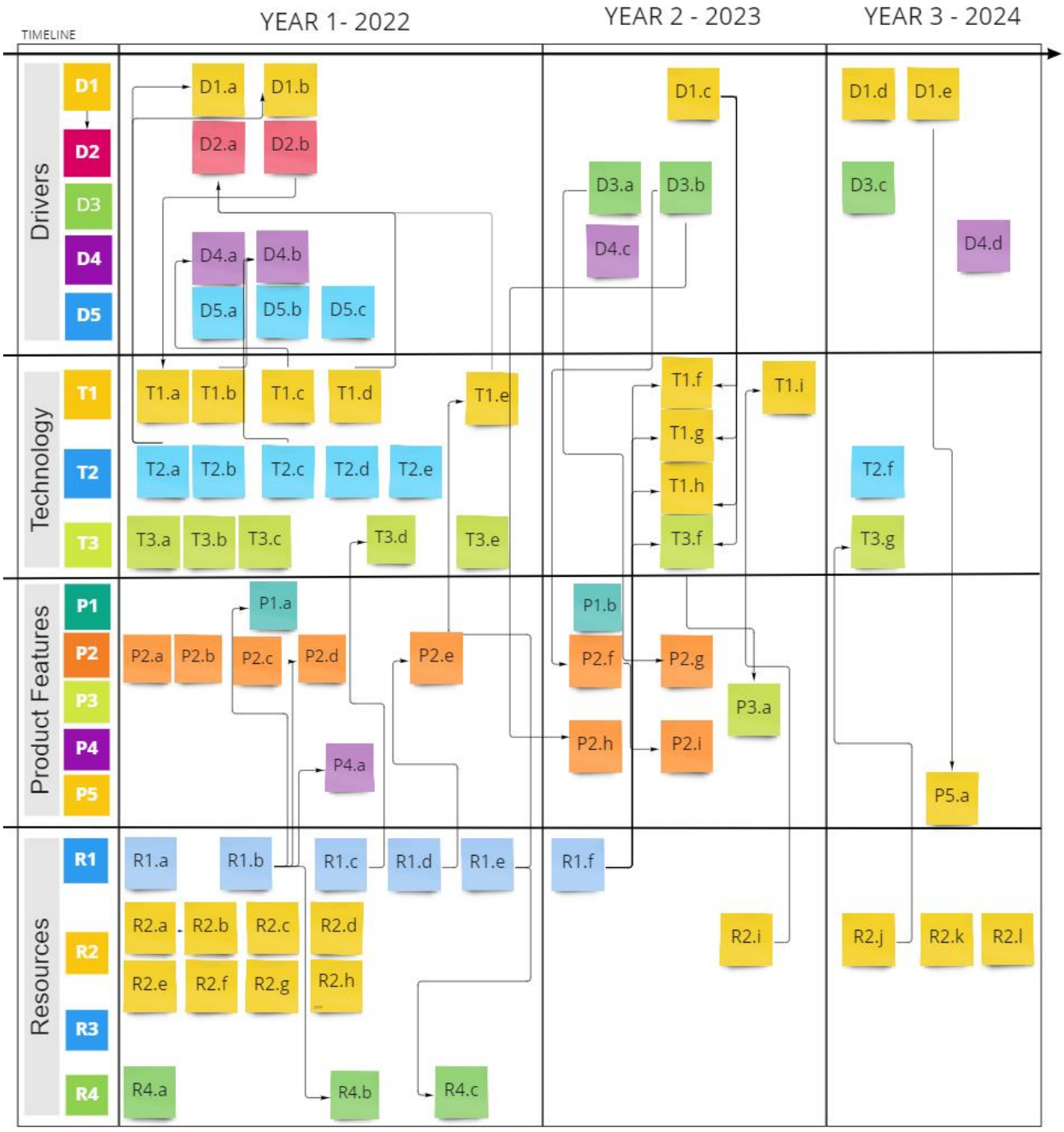


Figure 10: Technology Roadmap

1. Drivers

Drivers	D1	Technology	D1.a	Health trackers (Fitbit, Apple watch..)
			D1.b	Menstruation tracking apps
			D1.c	Health data mining by tech giants
			D1.d	Advanced use of AI and machine learning
			D1.e	Bodily monitoring technology
	D2	Government	D2.a	Roe vs Wade overturned
			D2.b	Concerns other Supreme Court cases will be overturned
	D3	Social	D3.a	Change in social views
			D3.b	Demand for virtual care
			D3.c	Election year
	D4	Economic	D4.a	Health care costs
			D4.b	Cost of data breach
			D4.c	Alternative source of revenue for health tech entities
			D4.d	Fines for non HIPAA Entities on health data breach
	D5	Safety	D5.a	Debate if abortion covered in life threatenin cases
			D5.b	Emerging Viruses (ie Monkeypox)
			D5.c	Ongoing CV-19 Pandemic

Figure 11 : Technology Roadmap: Drivers

The first roadmap section includes five drivers, which are the five sectors that were identified as holding the most impact on the need for health data cybersecurity, the first one being technology. There are currently a lot of technologies and devices that allow the tracking of health data. Big names include Fitbit, Apple watch, Garmin etc which include menstruation tracking apps. It is also projected that the health data mining by technology giants and technological advancement to include AI and machine learning as well as bodily monitoring technologies will factor into the health data collection.

The second driver, identified as governmental, was selected due to the very recent overturning of the Roe vs Wade ruling which removed the constitutional right to abortion. The fear of future supreme court cases being overturned that will impact health rights and that can be enforced through the collection of health data means that the need for advanced and solid cybersecurity is higher than ever. It is also imperative to tackle social drivers, as consumer needs keep evolving and changing. The expectation in the next couple of years is for the users of applications involving health data to increase, and the demand for virtual care to keep growing as it already has been due to the pandemic. The election in 2024 will therefore be impacted by voters looking for more security.

Economically speaking, current healthcare costs and costs of data breaches suggest the need for cybersecurity is already elevated. The sometimes-extravagant cost for healthcare should at least include data security, and data breach costs can be detrimental to entities with lower revenues. Projections for economic assistance to solve the issue includes an alternative source of revenue for health tech entities and fines for non-HIPAA entities. From a safety point of view, the current debate if abortion should be covered in life threatening cases as well as the ongoing Covid-19 pandemic as well as the emergence of new viruses such as monkeypox means that health data

privacy is in high demand as healthcare in general is becoming an even greater part of daily lives than before.

2. Technology

Technology	T1	Data Management	T1.a	Minimize data collection
			T1.b	Minimize links between data and individual users
			T1.c	Collect data securely
			T1.d	Store data securely
			T1.e	Ban data brokers from selling or transfering health and location data
			T1.f	Require enhanced record keeping of data use
			T1.g	Restrict data retention
			T1.h	Require data protection impact assessment for third party activities
			T1.i	Restrict government surveillance
	T2	Data visibility	T2.a	Clearly explain what data is collected and how it is used
			T2.b	Clearly explain how info is shared with others
			T2.c	Ensure data is not used in ways that can harm users
			T2.d	Ensure data is not used in ways that can harm users
			T2.e	Follow stated privacy policy
			T2.f	Publicy release data transparency report
	T3	Consumer Rights	T3.a	Allow users to control what data is collected
			T3.b	Allow users to review, correct, and export their own data
			T3.c	Allow users to delete content or terminate their account
			T3.d	Require government to obtain a court order before accessing consumer data
			T3.e	Comply only with valid demands for information
			T3.f	Require opt-in consent to data collection
			T3.g	Allow consumers to sue for data malpractice

Figure 12 : Technology Roadmap: Technology

The second roadmap section is about technology and how it is or should be affecting cybersecurity in health care. Data management first was one of the first subjects to be tackled. The idea of safe data management currently includes minimizing data collection, minimizing links between data and individual users, collecting and storing data securely, and banning data brokers from selling or transferring health and location data. In the future, the projection is that different processes will be needed for that same level of safe management of health data, including the requirement of enhanced record keeping of data use, restricting data retention, requiring data protection impact assessment for third party activities, and restricting governmental surveillance.

Data visibility is the main way data is available for the public and is therefore one the most straightforward ways for data to be used against consumers. Currently the ways to make that data safely visible is by clearly explaining what data is collected and how it is used and how the information is shared with others, and ensuring data is not used in ways that can harm users, notifying users of changes before they go into effect, and following any stated privacy policy. Hopefully in the future the addition of a data transparency report would also contribute to the safe visibility of healthcare data.

Consumer rights are the final subject tackled in the technology section. Giving the consumers power to control the usage of their private data should be a priority. Currently, that power is given to them through allowing them to control what data is collected, to review, correct, and

export their own data, and to delete content or terminate their accounts. Other processes include requiring the government to obtain a court order before accessing consumer data, and the right for consumers to only comply with valid demands for information. In the future, requiring opt-in consent to data collection and allowing consumers to sue for data malpractice will also add to that power.

3. Product Features

Product Features	P1	Dynamic Change	P1.a	Algorithm impact assessments
			P1.b	Authorized agents/ web browsers for opting out
	P2	Data Protection	P2.a	Firewalls
			P2.b	Authentication process
			P2.c	Netwrok security
			P2.d	Create a national "do not track" system
			P2.e	National standard to protect personal reproductive health data
			P2.f	Enhanced data inventory (RoPA)
			P2.g	Data deletion management
			P2.h	Compliance monitoring
			P2.i	Data restoration process
	P3	Effective Policy	P3.a	Provide means for consumer opt-in
	P4	Breach Response	P4.a	Penalties for executives that lie to the FTC
	P5	Inform Consumers	P5.a	Clarification of private and public health records

Figure 13 : Technology Roadmap: Product Features

Additionally, product features that are essential for the roadmap were identified. Technologies and processes are always on the path to change, therefore dynamic changes must be considered as part of the product features. Currently there are assessments for algorithm impacts on data, and in the future, the team projects the possibility of having opt out options for authorized agents in web browsers in order to safely keep up with ongoing changes.

Data protection is currently held out through firewalls, authentication processes, network security, national “do not track” systems and national standards to protect personal reproductive health data. Future protective practices will also include enhanced data inventory (RoPA), data deletion management, compliance monitoring, and data restoration processes. Under product features, future effective policy is expected, which would provide means for consumer opt-in. It will create a framework for a standardized permission requirement for users, and consensual sharing of data. Other future features include penalties for executives that lie to the Federal Trade Commission as a data breach response, as well as the clarification of private and public health records as part of informing consumers.

4. Resources

Resources	R1	Local Policy	R1.a	State-level policies proposed + passed: CCPA/ CPRA - CA, VCDPA - VA, CPA - CO
			R1.b	States pass the Mind Your Own Business Act (2019)
			R1.c	States pass the Fourth Amendment Is Not For Sale Act (2021)
			R1.d	States pass the My Body, My Data Act (2022)
			R1.e	States pass the Health and Location Data Privacy Act (MA, OR, WA, RI, VT)
			R1.f	State-level policies in-effect: CCPA + CPRA (CA), VCDPA (VA), CPA (CO)
	R2	Federal Policy	R2.a	Supreme Court Overturns Roe vs Wade
			R2.b	Comply with the Electronic Communications Privacy Act
			R2.c	Comply with the Health Insurance Portability and Accountability Act
			R2.d	Cosponsorship of the Net Neutrality and Broadband Justice Act of 2022
			R2.e	comply with the Video Privacy Protection Act
			R2.f	comply with the Children's Online Privacy Protection Act
			R2.g	Determine Value of Data
			R2.h	Women's Health Protection Act (2022)- H.R 3755 Passed the House
			R2.i	Federal expansion of ECPA (1986) to protect consumer data from govt surveillance
			R2.j	Federal expansion of FTCA (1946) to allow consumers to sue for abusive data practices
			R2.k	FTC require businesses to honor GPC
			R2.l	Comprehensive federal data protection policy, similar to CA, VA, and CO
	R3	Funding		
	R4	Organizations	R4.a	ACLU research and legislation to protect consumer data privacy
			R4.b	Hire 175 staff to police the private data market
			R4.c	Empower the FTC to create + enforce laws implementing policy

Figure 14 : Technology Roadmap: Resources

Lastly, different types of resources that have an impact on healthcare cybersecurity were identified. First are the local policies. There are currently many state level policies in effect that strive for the privacy and ethical use of healthcare data and many more proposed and passed and that are to take effect in 2023. Some notable policies include: the California Privacy Rights Act (CPRA), the Virginia Consumer Data Protection Act (VCDPA), and the Colorado Privacy Act (CO) which are all developing privacy compliance programs. There are also acts such as the "Mind Your Own Business Act", the "My Body, My Data Act" and the "Fourth Amendment Is Not for Sale Act" that have the same goal. They would protect citizens' privacy and allow consumers to control how their health data is sold and shared. "The Fourth Amendment is Not for Sale Act" and the Health and Location Data Privacy Act (MA, OR, WA, RI, VT) have similar goals where they stop data brokers from selling any personal information, such as location and health data, to law enforcement and intelligence agencies without legal permission.

Federal policies are a major resource for healthcare data security as well. There are a number of policies that are currently in place that enable safety and security regarding electronic personal data. The "Electronic Communications Privacy Act"or ECPA for example, protects electronic communication while they are being made up to the point when they are stored on computers. The "Health Insurance Portability and Accountability Act"or HIPPA, federally requires national standards creation and application to protect sensitive health information from being shared without the knowledge or consent of their subject. The "Video Privacy Protection Act" forbids the sharing of video records containing identifiable personal information. Another act worth mentioning is the "Children's Online Privacy Protection Act" or COPPA, which requires parental consent for collecting and using any personal information for children under 13 years old. Another important act that has passed the house in 2022, especially after the overturn of Roe vs

Wade is the “Women's Health Protection Act (2022)- H.R 3755” or WHPA, which would federally protect the right to access abortion care.

However, the need to expand some acts and policies such as the previously mentioned ECPA of 1986 and the “Federal Tort Claims Act” (FTCA) of 1946 - which allows consumers to sue for abusive data practices-, is still necessary for the success of those cybersecurity efforts, especially in order to keep up with the development and advancement of technologies and data sharing expansion. By also having the Federal Trade Commission require that businesses honor Global Privacy Control features, and by having a Comprehensive federal data protection policy similar to the previously mentioned California, Vancouver and Colorado acts, there are better opportunities to fulfill cybersecurity needs in the healthcare sector.

Lastly, there are current organizational efforts promoting cybersecurity in the healthcare sector, and those include research and legislation by the American Civil Liberties Union (ACLU) as well as proposed legislation by democratic senators. The ACLU Speech, Privacy, and Technology Project is advocating for legislation to protect consumer data privacy, as well as create a guide for businesses on how to better protect the privacy and free speech rights of individuals. [17] The Mind Your Own Business Act proposed by U.S. Senator Ron Wyden of Oregon, as well as other state senators, proposes means to better empower the Federal Trade Commission to create and enforce privacy protection, as well as act if laws are breached. If passed, the bill would establish minimum privacy and cybersecurity standards, issue serious fines for first offenders as well as criminal penalties for perjury, and create a system to facilitate consumers opting out of tracking, data sales, and targeted advertising - with provisions to waive fees for low-income consumers who qualify. The bill would also hire 175 staff members to police the unregulated private data market, and require corporations to assess the security, accuracy, and bias of their algorithms. A later draft of the Mind Your Own Business Act incorporates feedback, to provide better funding solutions for the proposal. The bill proposes revenue streams for the FTC through civil suits against companies that violate privacy regulations, then would allow redistribution of the funding to designated “watchdog” nonprofits that originally reported the violation. Tax penalties would also be levied on companies that lie about privacy protections. [32, 33]

VI. Conclusion & Limitations

This paper outlines the team's work to establish clarity on consumer healthcare data privacy gaps, research policy to enforce more effective consumer healthcare privacy practices, and create a roadmap to demonstrate how policy will influence the management of cybersecurity technology to better protect consumer healthcare data privacy. The technology roadmap outlines the evolution of cybersecurity technology through the key drivers, technology, product features, and resources that will impact consumer healthcare data privacy protection. The interactions of these factors are a key element of the roadmap. Policy will be a key catalyst in technology adoption. The resource element of our roadmap consists of local policy, federal policy, funding, and organizations. Local policy will begin driving change in product features, enabled by technology management in year one. Federal policy should expand these changes in year two. More strict enforcement of these policies, in regards to data breach response, is projected by year three, as well as the mass adoption of data security technologies propelling greater innovation in the industry. Data management and visibility technology features will interact with the economic, government, and technology drivers as explained through the policy proposals above.

Due to the dynamic nature of consumer data privacy public policy, our reference to academic literature in this area was limited. The lack of experience on the research team in specific cybersecurity technology management presented an additional limitation in the work which was constrained to eight weeks. Public policy is essential to enforce the implementation of this technology by corporations, but the research team recommends the development of a more comprehensive technology and product feature roadmap to provide clear guidelines for corporations striving to do the right thing to best protect their consumers before these policies are passed and enforced. The team recommends further research displaying the current privacy standards of corporations, to compare where these organizations stand on the spectrum of cybersecurity technology implementation and best practices - such as the "Easy-to-read Privacy Nutrition Labels" available on the Apple App Store [34]. Mapping major data breach response cases that have established precedent to enforce consumer data privacy policy, such as the $5 billion Facebook penalty, would provide more context on the trend of policy enforcement. Lastly, a more thorough economic analysis of the revenue streams driven by these policy changes would ensure the proposed standards are sustainable for non-profit organizations, government agencies, and the corporations which they will guide.

VII. References

1. Hill, K. (2022, June 30). Deleting Your Period Tracker Won't Protect You. The New York Times. https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html
2. Torchinsky, R. (2022, June 24). How period tracking apps and data privacy fit into a post-Roe v. Wade climate. NPR. https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps
3. Landi, H. (2022, February 1). *Healthcare data breaches hit all time high in 2021, impacting 45m people*. Fierce Healthcare. https://www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people
4. *2022-2026 Strategic Technology Roadmap* (Version 4 Summary). (2021). Cybersecurity & Infrastructure Security Agency (CISA). https://www.cisa.gov/sites/default/files/publications/STRv4_Summary_Public_Release_Final_20211123%20Updated%20508_1.pdf
5. Strielkina, A., Illiashenko, O., Zhydenko, M., & Uzun, D. (2018). Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment. 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), 67–73. https://doi.org/10.1109/DESSERT.2018.8409101
6. Ariu, D., Didaci, L., Fumera, G., Frumento, E., Freschi, F., Giacinto, G., & Roli, F. (2015). Yet another cybersecurity roadmapping methodology. 2015 10th International Conference on Availability, Reliability and Security, 719–726. https://doi.org/10.1109/ARES.2015.87
7. Al Omar, A., Jamil, A. K., Nur, Md. S. H., Hasan, M. M., Bosri, R., Bhuiyan, M. Z. A., & Rahman, M. S. (2020). Towards a transparent and privacy-preserving healthcare platform with blockchain for smart cities. 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 1291–1296. https://doi.org/10.1109/TrustCom50675.2020.00173
8. He, X., Alqahtani, S., & Gamble, R. (2018). Toward privacy-assured health insurance claims. 2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 1634–1641. https://doi.org/10.1109/Cybermatics_2018.2018.00273
9. Healthcare cyber security market size report, 2030. (n.d.). Retrieved August 14, 2022, from https://www.grandviewresearch.com/industry-analysis/healthcare-cyber-security-market
10. Schmidt, H. (2022, July 12). HIPAA Protection Slides Post-Roe, Healthcare Cybersecurity Under Siege. *Healthcare Exec Intelligence*. https://healthcareexecintelligence.healthitanalytics.com/news/hipaa-protection-slides-post-roe-healthcare-cybersecurity-under-siege
11. Data breach notification in the united states and territories | privacy rights clearinghouse. (n.d.). Retrieved August 14, 2022, from https://privacyrights.org/resources/data-breach-notification-united-states-and-territories
12. Rights (OCR), O. for C. (2009, September 14). Breach notification rule [Text]. HHS.Gov. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
13. Data breach response policies. (n.d.). Safety Net Project. Retrieved August 14, 2022, from https://www.techsafety.org/data-breach-response-policies

14. The state of consumer data privacy laws in the US (And why it matters). (2021, September 6). Wirecutter: Reviews for the Real World. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/
15. Build your roadmap to 2023 US privacy compliance. (n.d.). Grant Thornton. Retrieved August 14, 2022, from https://www.grantthornton.com/insights/articles/advisory/2021/build-your-roadmap-to-2023-us-privacy-compliance
16. Rahnama, H., & Pentland, A. "Sandy." (2022, February 25). The new rules of data privacy. Harvard Business Review. https://hbr.org/2022/02/the-new-rules-of-data-privacy
17. Privacy & technology. (n.d.). American Civil Liberties Union. Retrieved August 14, 2022, from https://www.aclu.org/issues/privacy-technology
18. Office for Civil Rights (2013) Summary of the HIPAA Privacy Rule, Health Information Privacy, Department of Health and Human Services https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#:~:text=The%20Privacy%20Rule%20protects%20all,health%20information%20(PHI).%22
19. Jane Thomason (2021) Big tech, big data and the new world of digital health, Global Health Journal, Volume 5, Issue 4, Pages 165-168, ISSN 2414-6447,https://doi.org/10.1016/j.glohj.2021.11.003. (https://www.sciencedirect.com/science/article/pii/S2414644721000890)
20. Dutcher and Zatkowsky (2021), Big Tech's Foray into Healthcare and Your Privacy, https://www.rochesterelderlaw.com/big-techs-foray-into-health-care-and-your-privacy
21. Drees J. (2020) The future of health data privacy: 6 things to know, Becker's Health IT https://www.beckershospitalreview.com/cybersecurity/the-future-of-health-data-privacy-6-things-to-know.html
22. Ravindranath M. (2020) What big tech companies aren't saying about HHS data rules, Politico, Ehealth https://www.politico.com/news/2020/01/10/big-tech-hhs-data-rules-097356
23. McGuire Woods (2021), FTC Issues Reminder on the Breach Notification Requirements by Health Apps and Other Connected Devices and Their Service Providers, mcguirewoods.com https://www.mcguirewoods.com/client-resources/Alerts/2021/10/ftc-issues-reminder-breach-notification-requirements-health-apps-connected-devices-service-providers#:~:text=Research%20from%20the%20Organization%20for,average%20of%20250%20per%20day.
24. Gershman J. (2020), Health Data After Covid-19: More Laws, Less Privacy, The Wall Street Journal https://www.wsj.com/articles/protecting-health-data-after-covid-19-more-laws-less-privacy-11599750100
25. McKeon J. (2022) How New Federal, State Laws Impact Healthcare Data Privacy, Health IT Security, xtelligent HEALTHCARE MEDIA https://healthitsecurity.com/features/how-new-federal-state-laws-impact-healthcare-data-privacy
26. Riggi J. (2022), The importance of cybersecurity in protecting patient safety, AHA Center for Health Innovation, American Hospital Association https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety
27. Reicin E. (2022), Protecting Consumer Health Data Privacy Beyond HIPAA, Forbes https://www.forbes.com/sites/forbesnonprofitcouncil/2022/05/10/protecting-consumer-health-data-privacy-beyond-hipaa/?sh=38bca3177b4e

28. A. Strielkina, O. Illiashenko, M. Zhydenko and D. Uzun (2018), Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment, IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2018, pp. 67-73, doi:10.1109/DESSERT.2018.8409101
29. D. Ariu et al. (2015), Yet Another Cybersecurity Roadmapping Methodology, 10th International Conference on Availability, Reliability and Security, 2015, pp. 719-726, doi: 10.1109/ARES.2015.87
30. Taylor, P., Allpress, S., Carr, M., Lupu, E., Norton, J., Smith, L., Blackstock, J., Boyes, H., Hudson-Smith, A., Brass, I., Chizari, H., Cooper, R., Coulton, P., Craggs, B.,Davies, N., De Roure, D., Elsden, M., Huth, M., Lindley, J., Maple, C., Mittelstadt, B., Nicolescu, R., Nurse, J., Procter, R., Radanliev, P., Rashid, A., Sgandurra, D., Skatova, A., Taddeo, M., Tanczer, L., Vieira-Steiner, R., Watson, J.D.M., Wachter, S., Wakenshaw, S., Carvalho, G., Thompson, R.J., Westbury, P.S., (2018), Internet of Things: realizing the potential of a trusted smart world, Royal Academy of Engineering
31. Koebler, J., & Merlan, A. (2022, August 9). This is the data facebook gave police to prosecute a teenager for abortion. Vice. https://www.vice.com/en/article/n7zevd/this-is-the-data-facebook-gave-police-to-prosecute-a-teenager-for-abortion
32. Wyden introduces comprehensive bill to secure americans' personal information and hold corporations accountable | u. S. Senator ron wyden of oregon. (n.d.). Retrieved August 15, 2022, from https://www.wyden.senate.gov/news/press-releases/wyden-introduces-comprehensive-bill-to-secure-americans-personal-information-and-hold-corporations-accountable
33. Wyden, colleagues introduce my body, my data act to protect reproductive health data | u. S. Senator ron wyden of oregon. (n.d.). Retrieved August 15, 2022, from https://www.wyden.senate.gov/news/press-releases/wyden-colleagues-introduce-my-body-my-data-act-to-protect-reproductive-health-data
34. Privacy. (n.d.). Apple. Retrieved August 15, 2022, from https://www.apple.com/privacy/
35. Ftc imposes $5 billion penalty and sweeping new privacy restrictions on facebook. (2019, July 24). Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook
36. Zhou, Yuan, et al. "A Policy Dimension Required for Technology Roadmapping: Learning from the Development of Emerging Wind Energy Industry in China." *2011 Proceedings of PICMET '11: Technology Management in the Energy Smart World (PICMET)*, 2011, pp. 1–9.