

Towards Medical Data Ownership by Patients: Implications,
Challenges and Solutions

Mohit Aggarwal



Declaration

I declare that the work described in this dissertation is, except where otherwise stated, entirely my own work, and has not been submitted as an exercise for a degree at this or any other university.

Signed: _____ Date: _____

Mohit Aggarwal



Permission to Lend and/or Copy

I agree that the Trinity College Library may lend or copy this dissertation upon request.

Signed: _____ Date: _____

Mohit Aggarwal



Acknowledgements

I cannot thank my supervisor Dr. Lucy Hederman enough. Without her encouragement, ideas, direction and critique, this work would not have been possible.

I am thankful to so many friends and colleagues. Their professionalism and inclination to change the world for the better is inspirational. For their participation towards this study, many of whom I met briefly while travelling. They enabled diversity of views and opinions which would not have been possible otherwise.

I want to thank facilities and staff of Trinity College Dublin and Bibliothèque nationale de France, where most of this work is written. And the course coordinators and teachers of Master's in Health Informatics in Trinity. I enrolled for learning more about use of technology in healthcare. But topics as diverse as cell functions, data standardization challenges, visit to hospitals and opportunity to talk to patients have been inspirational and opened a window into far wider spectrum of knowledge.

Lastly, I dedicate this work to my parents for encouraging me to take risks and being there to help recover from failures.



Abstract

Introduction

Medical data is economically valuable and there have been wide scale leaks and breaches in multiple jurisdictions. Role of insiders in these leaks have been significant. At the same time medical and external entities with access to patients' medical data act with much more discretion in areas of secondary usage and often prioritize monetization and consumer engagement. This study explores the possibility of medical data ownership by patients. It intends to act as an enabler for wider conversation in this regard. It takes a look at benefits, concerns and solutions towards this goal. And consider these themes in legal, economic and social settings.

Methodology

Comprehensive literature review is conducted to understand the existing landscape better and conduct a qualitative study with 16 participants. 10 non medical and 6 medical professionals. Emphasis is made to include a diverse set of non medical i.e. patient participants and to reach to a diverse roles of medical professional participants. Based on the literature review different set of questions for two groups with some overlapping questions were created. There underlying themes and observable patterns are identified and discussed.

Results

Research shows that there's a disagreement between two groups about who is medical data owner. Although medical professionals are legally owners, patients consider themselves as owners and have hosts of assumptions about their control. Both patients and medical professionals lack awareness on data leaks and data privacy laws. This might be a contributing factor towards high number of medical data leaks. The issue of secondary usage and implied consent for monetization and further sharing was raised by patients and concerns about selective sharing by patients were raised by medical professionals. Both groups contributed towards identifying solutions for medical data ownership that are shared in detail.

Conclusion

Implications, challenges and solutions for medical data ownership by patients were identified. It is acknowledged that there are number of glaring issues surrounding medical data ownership. It is also learned that it's a multifaceted problem with social, economic, legal and technical challenges. Current ownership regime is not ideal and more control should be granted towards patients. A need for avoiding an extreme is acknowledged.

Sections

1. Introduction	9
1.1 Preface	9
1.2 Background	10
1.3 Motivation	12
1.4 Research Question	17
1.5 Research Overview	18
1.6 Document Overview	18
2. Literature Review	21
2. 1 Introduction	21
2.1.1 Sources	21
2.2 Medical Data Ownership	21
2.2.1 Medical Data	22
2.2.2 Medical Data Entities	23
2.2.3 Data Ownership Definitions	27
2.2.3.1 U.S. Department of Health & Human Services	27
2.2.3.2 European Commission/Member States	27
2.2.3.3 GDPR	27
2.2.4 Medical Data Ownership by Law	28
2.2.4.1 United States	28
2.2.4.2 Canada	29
2.2.4.3 United Kingdom	30
2.2.4.4 European Commision/Member States	30
2.2.5 Conclusion	31
2.3 Implications of Medical Data Ownership by Patients	31
2.3.1 Patient Empowerment, Education, Autonomy and Wider Impact	32
2.3.2 Better Security and Privacy	34
2.3.3 Better Data Accessibility, Portability and Medical Care Choices	36
2.3.4 Conclusion	38
2.4 Challenges of Medical Data Ownership by Patients	38
2.4.1 Technical	39

2.4.2 Societal	39
2.4.3 Economical	40
2.4.4 Legal	41
2.4.5 Conclusion	41
2.5 Solutions for Medical Data Ownership by Patients	42
2.5.1 Open Data	42
2.5.2 Cryptographic Control	42
2.5.3 Law Changes	43
2.5.4 Conclusion	44
2.6 Medical Data Leaks, A Widespread Problem	44
2.7 Data Ownership Studies	46
2.8 Conclusion	47
3. Research Methodology	51
3.1 Introduction	51
3.2 Study Type and Rationale	51
3.3 Researcher's Positionality	51
3.4 Avoiding Bias	52
3.5 Methodology and Plan	52
3.5.1 Questions for Patients	53
3.5.2 Questions for Medical Professionals	55
3.6 Research Participants	57
3.7 Data Collection and Analysis	57
3.8 Ethical Considerations	58
4. Results	60
4.1 Participants Background	60
4.1.1 Patients Group	60
4.1.2 Medical Professionals Group	61
4.1.3 Participant Attributes	61
4.2 Contrasting Questions	62
4.2.1 Medical Data Ownership	62
4.2.2 Awareness of Medical Data Leaks	66
4.2.3 Awareness of Data Privacy Laws	69

4.2.4 Conclusion	72
4.3 Individual Highlights	73
4.3.1 Meaning of Medical Data Ownership	73
4.3.2 Benefits and Challenges of Medical Data Ownership by Patients	74
4.3.3 Misuse of Medical Data	75
4.3.4 Concerns and Attitudes Regarding Secondary Usage	77
4.3.5 Solutions for Medical Data Ownership by Patients	78
4.4 Emerging Themes	80
4.4.1 Control Over Secondary Usage of Medical Data	80
4.4.2 Commercialization For Wider Good	80
4.4.3 Selective Sharing of Medical Data for Insurance	80
4.4.4 Ownership With Education and Responsibility Awareness	81
4.4.5 Avoid the Monolith	81
5. Discussion	82
5.1 Interpretation of Results	82
5.2 Answer to the Research Question	83
5.3 Study Evaluation	84
5.4 Call for Renewed Patients Rights for Medical Data	85
6. Conclusion	86
6.1 Summary	86
6.2 Study Limitations	87
6.3 Importance of this Research	87
6.4 Opportunities for Future Research	87
6.5 Final Statement	88
7. References	89
Appendices	97
A. Abbreviations	97
B. Glossary	98
C. Figures, Tables and Charts	99
a. List of Figures	99
b. List of Tables	101

c. List of Charts	102
D. Ethics Approval Application	103
E. Interview Protocol	107
a. For Patients	107
b. For Medical Professionals	110
F. Information Sheet for Prospective Participants	112
a. For Patients	112
b. For Medical Professionals	115
G. Informed Consent Form	118
a. For Patients	118
b. For Medical Professionals	123
H. Ethics Application Proposal, Revisions and Approval	128
Research Purpose	128
References For Ethics Approval Application	129
Ethics Approval	130

1. Introduction

1.1 Preface

“After he was assassinated on Nov. 22, 1963, his family and the men who had served him continued the lying and began the destruction, censoring and hiding of Kennedy's medical records” - Richard Reeves - writer, columnist, lecturer

Who owns medical data?

Patients, doctors, governments? All of them? Some of them? None of them?

Today a lot is known about JFK's medical history [1]. It's not important to speculate the need for privacy for their medical data or what could have been the implications or challenges, if that was the case. It is important to take note that such a need was there in front of some of the most resourceful people and individual.

We may not give much thought about the implications and challenges about our medical data. But that doesn't mean there are no repercussions towards us [2]. Our existing medical systems and services are data troves. We are collecting and decimating more data than ever using hosts of complex and electronic systems. These improvements do provide us with better healthcare but they also expose us to new threats.

No system is ideal. Some solutions are perceived to be cumbersome and compromising of users' experience in terms of giving them more responsibility and information. These conclusions may seem intuitive but for the health and well being of patients the opposite is true [3].

I finally end this section with two quotes. The first is related to medical insurance law and the second is about maintaining the technical status quo. As we explore the solutions, awareness of both of these factors become important. Healthcare sector's move towards embracing EHRs has been a leap forward. But these very systems have made hospitals targets for medical data breaches and could be preventing us from moving towards better, more secure systems that can provide better healthcare through patient empowerment and education.

“The fact is that a bill allowing any employer to deny insurance coverage based on a moral objection along with giving an employer permission to ask for medical records showing why a woman is taking birth control opens up a set of problems that I'm sure its

sponsors have not fully considered” - Richard Carmona - physician, nurse, police officer, public health administrator, and politician

“Hospital and healthcare software security can always be marginally improved, but if we want to lower the risk of healthcare security breaches, we need to take a very different approach. Only marginal improvements can be made by investing in more of the same resources in the problem, and the [return on investment] has diminishing marginal returns. A better approach is to understand the root causes at the core of healthcare security breaches” - Ron Avignone [4]

1.2 Background

“Data is the New Oil” - Brian Krzanich - CEO, Intel Corp.

Oil’s value as a resource cannot be understated in context of industrial revolution. If data is the new oil, *how valuable would medical data be?* Indeed it is considered highly valuable and priced higher than financial data [108].

Having underscored the economic incentives, it should be highlighted the sheer amount of medical data leaks and breaches, social and economic repercussions on people affected and lack of public awareness on this issue [21][26].

This research starts with a hypothesis that **medical data ownership by patients can prevent and reduce the scale of these issues**. It aims to identify the implications, challenges and solutions towards that end.

It takes a wider look at the term patient and refer to general public i.e. anyone who has been a patient or have been a user of medical services by this term. Medical professionals are not excluded from this definition. Their experience, knowledge and everyday concerns presents an alternate and valuable view of the system that involves all of us.

Every data breach adversely affects the entity responsible for its storage and security **both in public trust and costs**. Figure 1.1 below taken from 2017 study on Cost of Data Breach, done by Ponemon Institute and sponsored by IBM Security lists cost per capita of data breach across various industries. It highlights healthcare costs have been the highest for past four years and were highest in 2017 as well [110]

Per capita cost by industry classification

*Historical data are not available for all years

Measured in US\$

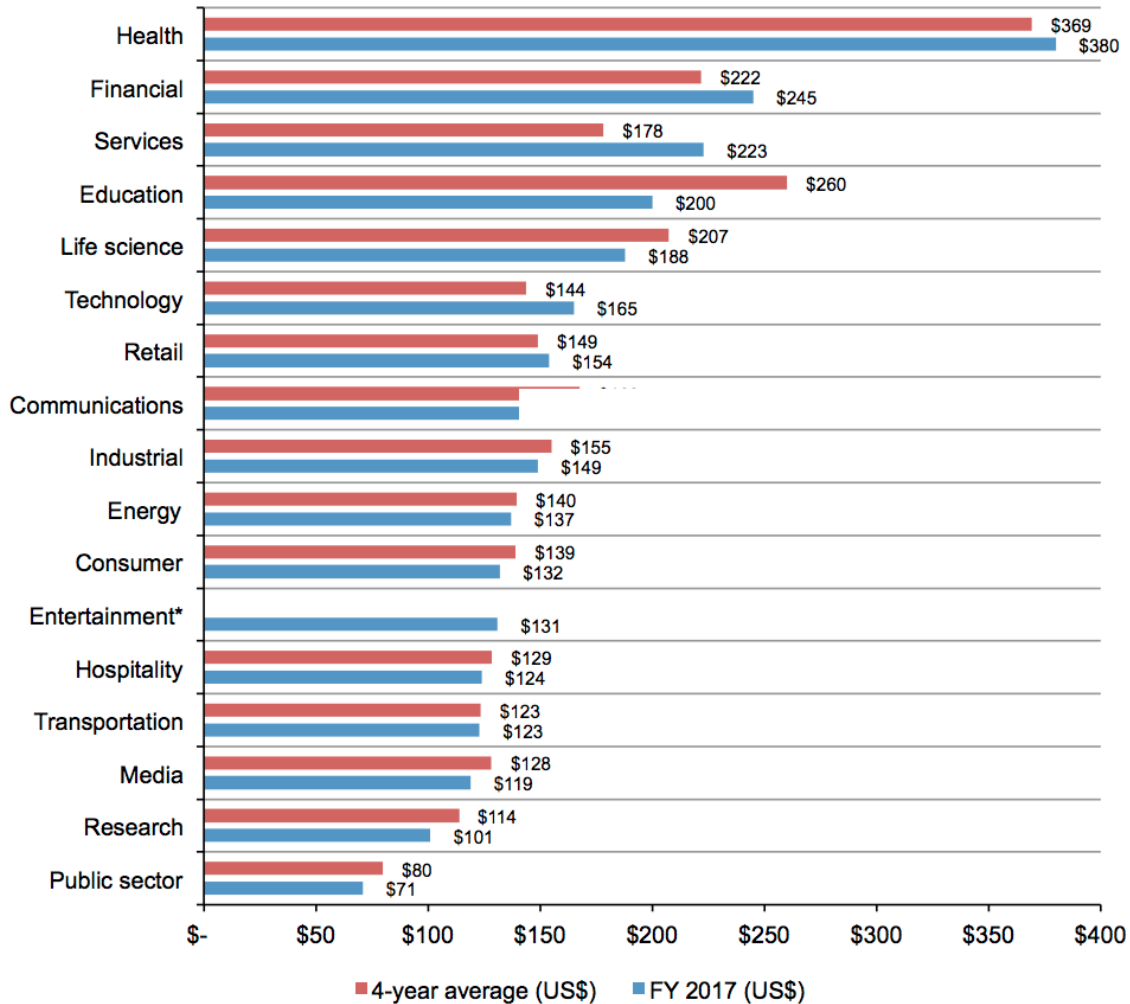


Figure 1.1 - cost of data leak per capita, 2017 [110]

Number of changes have been made in recent years towards patient centric care, patient empowerment and education. And these changes have made healthcare better by shared decision taking and raising patient engagement. That has resulted in improved health outcomes. With advent of electronic systems, portability and interoperability of medical data between devices and facilities. Patients being mobile, self educating and generating medical data using wearable devices. It becomes important that sharing constraints, authorizing roles and ownership of medical data is raised at the right forums.

This research aims to act as a value add towards this goal.

1.3 Motivation

“Mr. Zuckerberg, would you be comfortable sharing with us the name of the hotel you stayed in last night?” - Dick Durbin, United States Senator

“We didn’t take a broad enough view of our responsibility and that was a big mistake. And it was my mistake.” - Mark Zuckerberg, CEO, Facebook

A 2012 study highlights that as much as 30% of all stored data in the world is generated in healthcare industry [111]. In 2017, in US alone more than 450 data breaches have been reported to affect 5.5 million patients, a number that stands at 173 million, if counted since 2008 [28][112]. Insider wrongdoing is identified as root cause of biggest breach in 2017.

These are staggering numbers. With long term social, economic and health repercussions on affected patients. Nor well publicised neither considered worthy of wide scale alerts. While human error is noted as being the cause of 28% of the medical data breaches. There’s a **notable contrast** where organizations and businesses perceive employee negligence to be the biggest concern for medical data leak but consider IT departments to be accountable for incident responses [110][113].

Figure 1.2 below highlights root causes of data breach in 2017 study. It identifies 28% as human errors and 27% and 47% as system glitch and criminal attack respectively. Malicious insiders as highlighted in Figure 1.3 and 1.4 are noted as perceived threats. It can be concluded that some of the breaches could have been caused by known personnels.

Distribution of the benchmark sample by root cause of the data breach

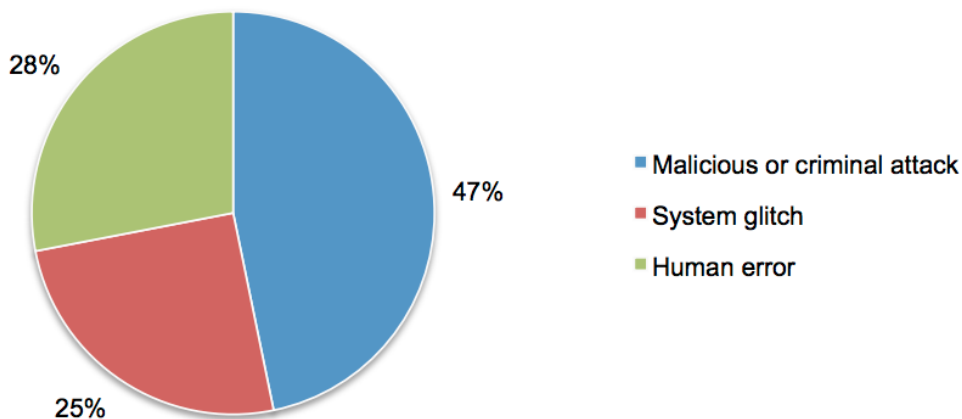


Figure 1.2 - root cause of data breaches, 2017 [110]

Figure 1.3 and 1.4 below highlights security threats that healthcare organizations and business associates worry about the most. It is notable that employee negligence is ranked highest in both. Also somewhat related, malicious insiders and employee owned mobile devices rank high in the list. Figure 1.4 highlights the departments that are perceived as accountable for data breach incident response. It is notable that organizations ranks corporate compliance higher than business associates in this list. And latter consider information technology and security to be higher as compared to organizations.

Security threats healthcare organizations worry about most
 Three responses permitted

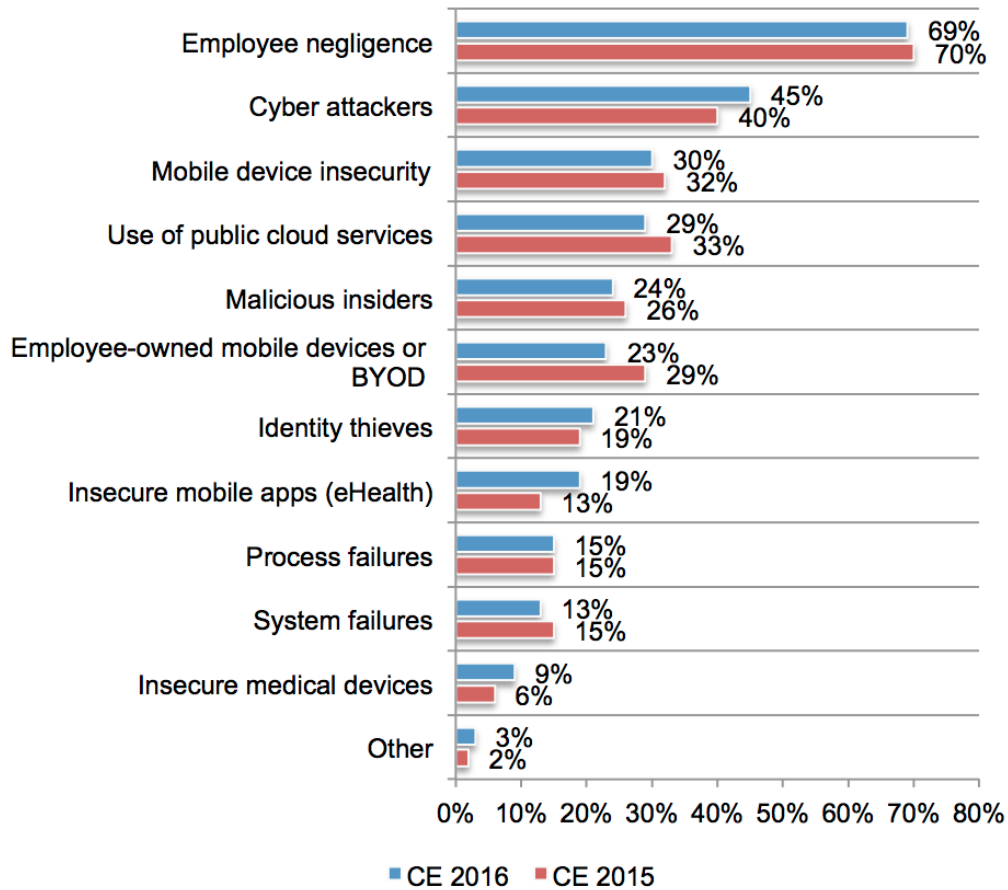


Figure 1.3 - security threats that worry healthcare organizations, 2016 [113]

What security threats worry business associates the most
 Three responses permitted

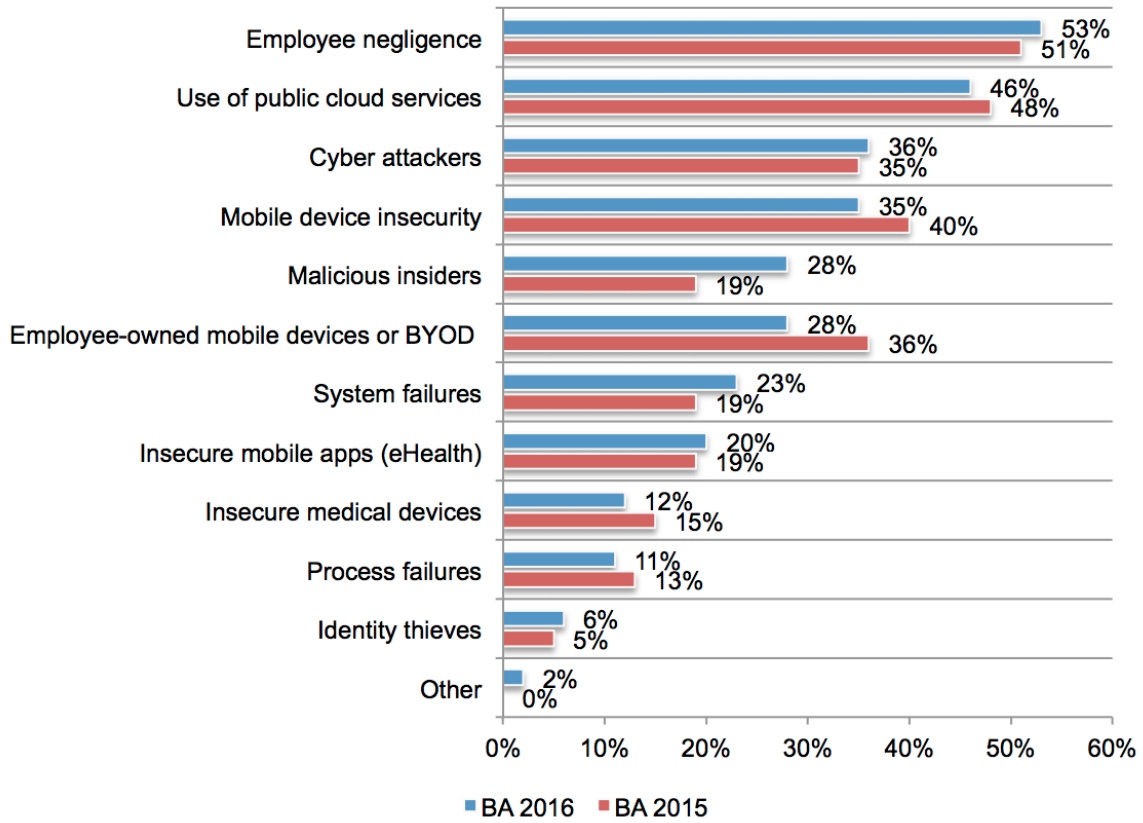


Figure 1.4 - security threats that worry business associates, 2016 [113]

Which department is ultimately accountable for the data breach incident response?

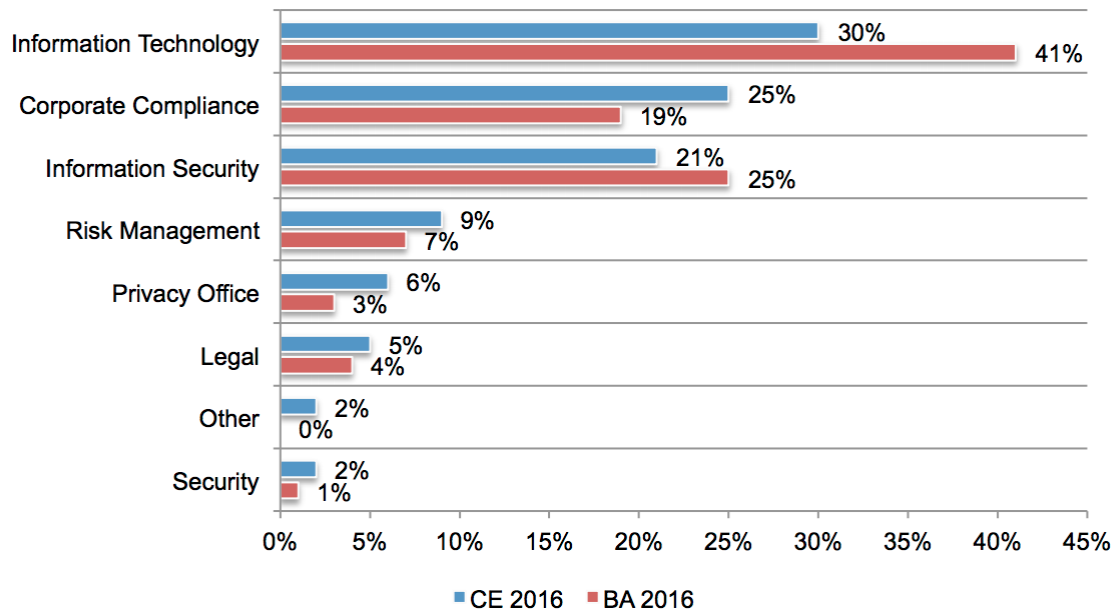


Figure 1.5 - department accountable for data breach incident response, 2016 [113]

Medical data sharing is an important aspect of modern healthcare systems. It brings lots of value addition for research and medicine. And everyone benefits in the long term. But reality does not confirm this. In truth, because of medical data being economically viable, data is shared for hosts of invisible reasons with external entities. There are also issues reported about what termed as **medical data blocking**. Where one entity withhold medical data for economic gains, placing patients health secondary [37][38].

In a comprehensive data privacy and consumer autonomy study [115], it is postulated that consumers are not adequately empowered. They share more data than preferable. Low level of trust in governments and other data entities is noted.

Concerns around data ownership also extends to secondary usage of data. Companies collecting consumer data in silos can be acquired and merged. Given enough parameters, patient identities can be deanonymized [3]. Preliminary research suggests people’s willingness to share data to further research. But they may not be fully aware of concerns this presents.

Following issues are broadly identified with the current policies and practices

1. Data sharing and access
2. Data security and breaches

3. Accountability and public awareness
4. Secondary usage and commercial incentives

All of these issues revolve around the question of **medical data ownership**.

Motivation for this research comes with the intent and knowledge that current system and policies, although brought forward with good intent and have resulted in hosts of advantages; causes undue harm that **can be prevented with some difficult choices**. Choices that are difficult not because of economic or technical investments required but largely due to incorrect incentives that makes the question of medical data ownership all the more important. Currently healthcare organizations act as data owners and unintentionally creates hosts of security, privacy and misaligned incentive issues.

1.4 Research Question

The aim of this study is to answer the following question and understand the following related issues


What are the implications, challenges and solutions for transferring medical data ownership to patients?

The question raises hosts of follow up and related questions

- What is the meaning of data ownership and medical data ownership?
- Who are the current medical data owners and what issues are being caused due to this?
- What are the general attitudes and awareness about medical data ownership i.e. is everyone in agreement on ownership?
- Does patients know the medical data privacy laws?
- Does medical professionals knows medical data privacy laws?
- Are patients and medical professionals knowledgeable about the scale and social repercussions of medical data leaks and breaches?
- How do these answers vary between geographical, social and economic divides?

Ownership as an abstract concept encompasses social, legal and economic spheres. It is by extension also an awareness issue. And can have wider effects when the ownership changes legally. Although this study is limited in terms of user participation. All these questions and their answers are related and should aid towards answering the primary question.

Outcome of this research should elucidate

- 
1. Known concerns and challenges around data sharing and ownership
 2. Users understanding of medical data ownership, privacy laws and misuse of such data
 3. Professionals understanding of medical data ownership, transfer and access
 4. Highlighting and identifying solutions and concerns in empowering users towards medical data ownership

1.5 Research Overview

Preliminary research helped identify scope and various facets of medical data ownership. Based on it, research question and related questions presented in section 1.4 were formed. It also underscored conclusively that **this is not a technical problem and is multifaceted**.

Based on this, search terms are identified and comprehensive literature review using research papers, existing studies, web, news, journal search and brief understanding of data and medical laws is conducted.


Based on the literature review, research questions, methodology, interview protocols, selection of participants are identified. A comprehensive ethics approval application was made to Trinity College Dublin with interview protocol, information sheet and informed consent form for both patients and medical professional groups. These documents are included as Appendices D, E, F and G. Ethics application has undergone multiple reviews and concerns regarding anonymization of participants identity, ability for them to not be recorded were addressed. Original proposal, revision history and approval email can be seen in Appendix H. Section 3.6 (Research Participants) and Section 3.7 (Data Collection and Analysis) were included in ethics approval application as well.

It become apparent from literature review that diversity from general public group and varying roles from medical professional group will be crucial for the study. Selection of participants was made with this consideration. Each group has related but different set of exploratory questions that helps highlight the contrast in medical data ownership. Interview Protocol (Appendix E) lists these questions. Section 3.5 (Methodology and Plan) lists all questions for both groups and rationale for inclusion.

1.6 Document Overview

This document is divided into following sections

1. **Introduction** : Highlights the background, motivation, formulation of research question, research and document overview. The section aims to underscore why the question of medical data ownership by patients is of importance by briefly presenting facts and known issues with current ownership regime.
2. **Literature Review** : This section goes in depth towards finding answer to primary research question i.e. to identify implications, challenges and solutions for medical data ownership by patients. It highlights various data entities, their lawful rights and interactions. It explores wider areas based on related articles towards patient empowerment, engagement. It also highlights hosts of issues with current system that can be addressed by targeting medical data ownership. It also takes a brief look at data sharing studies and present their findings. Every section in literature review has its conclusion with final conclusion summarizes everything as a comprehensive whole.
3. **Research Methodology** : This section highlights the research methodology, participant groups, ethical considerations and overview of questions posed and their rationale.
4. **Results** : This sections goes in detail about emergent themes and highlights participant responses towards those. It identifies patterns as learned from the interviews. It presents some quotes and findings and highlights socio, economic, cultural and role based differences between participants. It also puts patients and medical practitioner responses in contrast to understand underlying themes better.
5. **Discussion** : This section highlights primary outcomes from research results and learnings from literature review in context of research objective and related questions.
6. **Conclusion** : This section contains the author's conclusions based on literature review and research. It includes importance of this research and highlights known shortcomings. It also includes recommendations for potential future research areas and suggestions for researchers.
7. **References** : Numbered list of references. References are research papers, news, business studies and journals

- 
8. **Appendices** : Abbreviations, Glossary, List of Figures and Tables, Ethics Application, Interview Protocol and related forms

2. Literature Review

2.1 Introduction

This chapter presents the literature reviewed for this research. It details implications, challenges and solutions about medical data ownership by patients. In that spirit, it places patient at the center and explores these areas with them having **authority, control and responsibility**. It lists various studies and identifies pitfalls that could have been avoided or better handled with patients as medical data owners. The literature review cannot be deemed complete without highlighting the need for this. Towards that, sections about medical data breaches, incentives and privacy laws are included. Medical data ownership is a more complex and challenging form of data ownership. Underlying laws and society's awareness of them is important to understand the complexities around medical data security and thus ownership.

2.1.1 Sources

The following search terms were used in Trinity's Stella Catalogue and Google Scholar. Full text of relevant articles identified through Scholar was obtained through Stella Catalogue.

Search Terms: Data Ownership, Medical Data Ownership, Medical Data Leaks, Medical Data Protocols, Data Privacy Laws, Health Data Leaks, Preventable Deaths Medical data, Shared Decision Taking

Some articles from reputable publications and reports from corporations are also cited for recent statistics.

Some articles from British Medical Journal and Global Health are cited for highlighting and understanding medical data ownership issues on wider setting

Existing national data privacy laws like GDPR, HIPAA, HITECH, Irish, French, German DPAs that are precursor to GDPR were referenced at a high level

2.2 Medical Data Ownership

This document started with the question (Section 1.1). *Who owns medical data?* This section aims to elucidate on the meaning of medical data ownership. It starts with identifying what constitutes medical data. Could it be that multiple entities and individuals can be shared owners? Any

solution needs to adequately empower all entities to perform their primary responsibilities. Knowledge of these entities and their ownership requirements is critical for the following sections.

2.2.1 Medical Data

Medical systems and services and related entities deal with large amount of data. Before delving into medical data ownership by patients, it is important to understand who are the producers and processors of medical data.

The following broad categories of medical data producers and processors can be identified

1. Patients
2. Clinicians
3. Medical Services
4. External Entities

Table 2.1 lists some of the data for the above categories

Patients	Clinicians	Medical Systems	External Entities
<ul style="list-style-type: none"> ● Personal Health Records ● Consumer Medical and Health Device Data 	<ul style="list-style-type: none"> ● All medical records (charts, x-rays, summary reports) ● Prescriptions ● Clinical studies 	<ul style="list-style-type: none"> ● Automated data analysis and reporting services ● Metadata 	<ul style="list-style-type: none"> ● Genome sequencing services ● Insurance companies ● Data aggregators

Table 2.1: categories of medical data

There could be other data which may not be considered medical in itself but if it is used to derive medical or health outcomes for a person, it can be considered as medical usage of such data. It should be noted that all this data is either about the person or metadata of the data that is about them. Table 2.2 lists broad relationship between medical data, authorizer for data extraction, data processor and data consumer.

Medical Data Type	Authorizer/Creator	Processor	Consumer
Personal Health	Patient	External Entity	Patient/External

Records			Entities
Medical Records	Clinicians	Medical Systems	Clinicians
Metadata/Reports	Medical Systems	Medical Systems	Clinicians
Genomic Data	Patient	External Entity	Patient/External Entities
Big Data	External Entities	External Entities	External Entities

Table 2.2: Relationship between medical data type, data creator, processor and consumer

The term Big Data here is used to refer to aggregating, processing and assimilating unrelated patient data to derive medical conclusions from it. For example aggregating patient's sleeping data with their spending habits to derive conclusions on their mental health. Case of External Entities is contentious and notable. In a recent report, Facebook made multiple attempts to access anonymized patients' medical records [56]. It should be noted that there are known procedures and attacks that can deanonymize the datasets [57] [58].


2.2.2 Medical Data Entities

Looking at the legal framework, broadly three entities can have requirements and rights for medical data

1. Individual i.e. patient
2. Clinicians, hospital
3. Government

There are certain entities and platforms that have no legal status but store and process medical data. These platforms do that through user consent and provide services in terms of recommendations, alerts and integration of medical data from multiple sources. Some examples are Google Healthsuite, 23andMe, iOS Health etc [9][10]. Some of these services provide Health Insurance Portability and Accountability Act (HIPAA) compliant cloud services [8] and other added services for medical data processing, aggregation, management and analysis **without legal standing**. Some services are future oriented and their data collection and analysis is regarding human genomics. In that regards they stand to benefit from patient data. *But do they have legal standing to do this and are patients adequately informed about secondary usage?*

Figure 2.1, 2.2, 2.3 and 2.4 lists screenshots of some of the medical products and their data storage and processing offerings by leading commercial entities. Further secondary usage and sharing is a legal gray area. Some products may not have legal compliance and package



themselves as consumer apps rather than medical aids. For e.g. Apple Health works as a secure health data store. It can interface and integrate with third party devices and apps and allows access to user generated data on authorization by user. *How trusted and compliant are these third parties?*

Similarly, 23andMe collects genomic data which can easily identify an individual. Most passports and national IDs are biometric. *How far can secondary sharing go?*

Give patients fast, efficient service while meeting the strict requirements of regulations like HIPAA.

Provide HIPAA-compliant access to patient information.

- Store patient data files in a [HIPAA-compliant repository in Google Drive](#).
- Use Google's mobile device management and encryption to keep the data secure.
- Allow authorized employees to access the information from any corporate-managed device.



Figure 2.1 - Screenshot of G-Suite for Healthcare offering by Google



Explore HealthVault

Discover apps & devices

Sign up or sign in →

Take control of your health.

Explore HealthVault →

What is HealthVault?

Microsoft HealthVault is a trusted place for people to gather, store, use, and share health information online. [Learn more](#)

Organize your family's health information.

Be better prepared for doctor visits and unexpected emergencies.

Create a more complete picture of your health, with you at the center.

Achieve your fitness goals.

Figure 2.2 - Screenshot of Microsoft Healthvault product by Microsoft

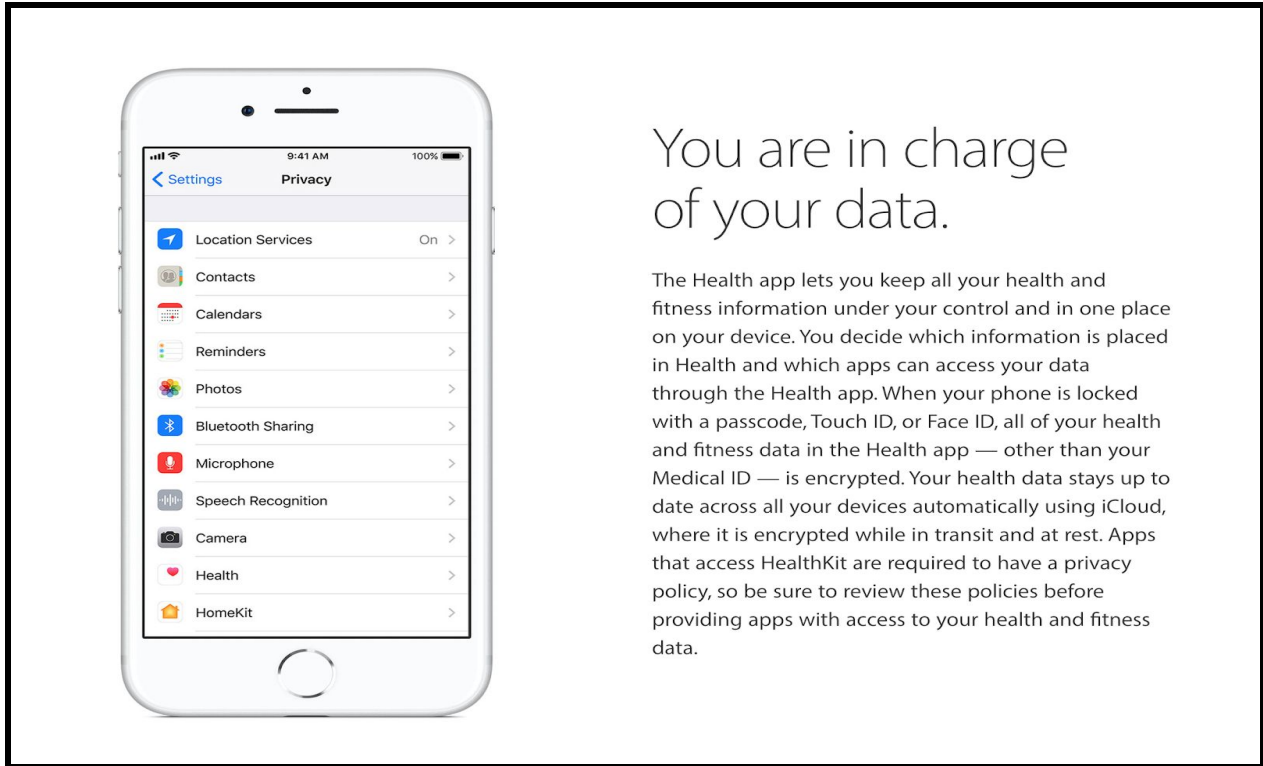


Figure 2.3 Apple Health is a comprehensive health data platform by Apple



You have new DNA Relatives

Dear _____

6 people who share DNA with you have joined DNA Relatives over the past 59 days.

[Visit DNA Relatives](#)

Figure 2.4 - 23andMe is a genome sequencing service with investments from Google

With understanding of various entities involved, let's take a look at the meaning of **data ownership** as defined by some reputable sources

2.2.3 Data Ownership Definitions

2.2.3.1 U.S. Department of Health & Human Services

Guidelines and definitions of data ownership are detailed from a researcher's perspective and needs [10]. Various boundaries, ethical and legal concerns are highlighted. This becomes important and of use in secondary usage of medical data. The following definition is taken from [10]

Data ownership refers to both the possession of and responsibility for information. Ownership implies power as well as control. The control of information includes not just the ability to access, create, modify, package, derive benefit from, sell or remove data, but also the right to assign these access privileges to others (Loshin, 2002).

2.2.3.2 European Commission/Member States

A detailed study of various member states' laws was published under the title "Legal study on ownership and access to data" [11].

The study notes various viewpoints in data ownership around trade secrets and contracts between commercial entities. Many countries have expressed interest in disallowing data hoarding, allowing access to public data and individual's control over their data. Individual **data ownership is not clearly defined** although some rights regarding individual health data are ascertained (Section 2.2.4.4).

2.2.3.3 GDPR

GDPR is a European regulation, introduced in May 2018, that defines various terminologies, rights and framework related to 'personal data' and 'data subject' (natural person). It's easier to draw parallels from this towards medical data. But it should be ascertained that they are related but different [12][13]. The law states

*'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the **physical, physiological, genetic, mental**, economic, cultural or social identity of that natural person;*

A GDPR definition related to secondary usage of data is as follows

*'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, **health**, personal preferences, interests, reliability, behaviour, location or movements;*

GDPR defines the limits, reach and penalties for misuse of personal data. It does not define data ownership but defines constraints, checks and balances regarding how someone's personal data be processed and shared further. In that respect **definition of data ownership can be inferred in respect of treating it as someone else's property.**

With some knowledge of broader data ownership and related definitions and concerns, let's look at the national laws related to medical data ownership

2.2.4 Medical Data Ownership by Law

2.2.4.1 United States

Figure 2.5, taken from [6], shows clearly that only one US state has legally made patients owners of their data. Others either have no legislation or have deemed hospitals or physicians as owners.

Physicians generally do not need express consent to include patient health information in an eRecord, or to share patient information with other healthcare providers for the purpose of providing treatment. Privacy legislation also generally permits custodians to share personal health information with an agent or affiliate on the basis of implied consent - CMPA, Electronic Records Handbook [15]

Question about ownership of records is answered on CMPA's website at [16], which states that **information belongs to the patient but the record belongs to the person or organization who created it.**

Custodians are also required to keep all records for the minimum of 15 years, thereby not allowing right of removal.

2.2.4.3 United Kingdom

The UK House of Commons Library lays down a good review of existing legislations and future vision for accessibility and rights to access of patients records with multiple entities and circumstantial exceptions (2015) [18]. Although a past ruling (1976) [19] places authority of patients' records under NHS as property of Secretary of State and grants discretion to medical professionals regarding access to records. In this context it is important to note the overall change over the years.

By the end of 2014, 21% of patients across England could access their records online. This number and further information access to patients has increased over the years and vision is laid down to increasing sharing with other entities. It should be noted that hospital records are retained for a minimum of eight years, whilst GP records are retained for a minimum of 10 years.

Further Caldicott Principles [20] are referred to as guiding rules regarding handling and sharing of patient data with different entities and amongst entities.

These guidelines and principles once again places rules and responsibilities with hospital staff and medical entities.

2.2.4.4 European Commission/Member States

Same study referred to in Section 2.2.3.2 [11] lists some rights regarding individual health data

Under Belgian and under UK data protection and healthcare laws, an individual has the right to gain access to any personal data pertaining to him/her, held by a company or other individual.

Under Dutch data protection and healthcare laws, an individual has the right to gain access to any personal data pertaining to him/her, held by a company or other individual

2.2.5 Conclusion

“One of the tenets of Data Governance is that enterprise data doesn’t “belong” to individuals. It is an asset that belongs to the enterprise. Still, it needs to be managed. Some organizations assign “owners” to data, while others shy away from the concept of data ownership” - The Data Governance Institute

Many articles summarize patients as medical data owners when referring on national level, reality does not reflect that [5][6]. HIPAA (in the US) has **no concept of data ownership**, it deals with rights to access and amendments [7]. State laws stand clearly towards hospital and clinicians as owners.

It is worth noting that there’s no clear legislation towards medical data ownership. In many places **implied consent** is assumed and entities are authorized to grant access to third parties and to other entities. Many legislative bodies have granted patients access to their data. But ownership is still not with them. This safeguards and enables commercial and system interests. And although perceived to be aiding patients, this works against them with **41%** of data leaks happening due to insiders [27].

Following sections will explore challenges, implications and solutions for medical data ownership by patients.

2.3 Implications of Medical Data Ownership by Patients

By gaining access to their own data, people could use it with information about themselves from other sources in order to create “rich data” – a far more valuable commodity than mere “big data” - Tim Berners Lee, inventor of world wide web

The previous section has clearly underscored that although medical data or data used for medical reasons is either about the patient or is metadata about patient’s data, its lawful ownership does not reside with them. That causes privacy, security and sharing concerns [37] that prevents a better healthcare system. Having established that current system is far off from its stated goals, this section explores the implications of medical data ownership by patients

2.3.1 Patient Empowerment, Education, Autonomy and Wider Impact

Economic incentives of ownership cannot be ignored and that ties with pursuit of happiness. Data ownership by patients should not merely address accessibility. That data should be owned and controlled by them. There are parallels between property ownership, its value in creating economic prosperity and data ownership. **Without ownership, there can be no trusted exchange** [38]. A counter view to above arguments highlights that different assets should have different forms of ownership [42]. **Medical data's ability to be useful as a collective resource does separate it from property** but it doesn't alleviate calls for ownership by patients. Patients themselves want their data to be shared to further research [43]. Technological solutions can make the former possible and enable the latter [41]. Multiple government reports suggests there is a system wide issue in data sharing [37][40]. This renews calls for patient empowerment. Current system considers patients at data generators. It bounds them to types of data they can generate and is admissible.

Would it not be feasible if patients, given indications and education about their ailment can, if they want to, explore alternative medical options and generate medical data i.e. acceptable by the health system?

To draw a parallel to this, the episode of medieval Europe where climate change resulted in 20% population reduction. At the heart of this calamity was crop loss. If peasants were allowed autonomy over what to grow and methods to grow them, that would have allowed upto three times as many people to be fed [92]. 21st century call for move to Agroecology, which relies on farmers' knowledge and experience of their ecosystem to maximize yields echoes this [93].

Multiple studies highlight significant improvement in patient's health with increase in engagement. Positive effects of early treatment and intervention in managing chronic diseases are widely recognized [44]. Patients with access to doctor's notes report better medication adherence [55]. Studies also indicate patients' higher willingness to share data than physicians.

At the same time companies are concerned less about research potential than about **customer engagement**. These studies highlight that patients are concerned about unintended use of data and want better control and ways to express consent [45][46]. Sweden aims to give its citizens electronic access to their medical records by 2020. Over a third of population already have accounts and studies show patients with such access are better educated about the illness and treatment is more successful [52].

Clinicians and healthcare system overall can benefit from more informed patients [3]. From seeking interventions proactively to better engagement in clinical settings, is possible through patient education. Studies show that access to clinician's notes after appointments encourage

individuals to improve their health, results in shared decision taking and better engagement. [3][49]

Wider impact of more in control and aware population are worth highlighting. There are many new research platforms that aims to collaboratively and through wider participation address some pressing issues like climate change, loss of biodiversity, ocean acidification etc. It is noted that these all have potential to adversely affect health [69]. Study notes that despite profound implications, relatively little research has been funded on global environmental change and health. The Rockefeller Foundation-Lancet Commission on Planetary Health identifies three barriers to action as

1. empathy failures (economic growth neglecting future health effects of environmental degradation),
2. **knowledge failures** (research and information challenges)
3. **widespread inability to use research evidence** effectively and systematically within decision making frameworks.

More empowered patients who have better control and awareness of their health data would be better collaborators and can act as counter to strong vested interests (highlighted as an enabler for third barrier listed above).

Citizens' juries have increasingly being used in government decision making including health policies. Recently (in 2018), Ireland passed abortion referendum by public vote. But a representative citizens group of 99 strangers formed in 2016 made the recommendation to the Irish government to permit abortion in early pregnancy [70]. A population that is more in control of their medical data and understand the responsibilities and concerns around it can catalyze and aid in creation of better policies. Calls are already being made to put health at the heart of **all policy making** [68]. Furthering the point for more control and awareness of patients regarding medical data.

There are many opportunities for SDM (Shared Decision Making) where scientific uncertainty exists. In these situations patients make their decision from both objective information available and subjective viewpoint. A 2017 Study regarding SDM for Influenza Vaccination notes that point is not to oppose influenza vaccination but that currently available scientific data should be analysed and that the right information be given to patients. It asserts that responsibility of health programmes must be separated from the responsibility for making information tools. Furthermore patients should always be included in creation of communication tools in health care [85].

2.3.2 Better Security and Privacy

“Medical devices and EHR systems are notoriously vulnerable to remote compromise” - James Scott, Senior Fellow, Institute for Critical Infrastructure Technology

Current system with implied consent on ownership of medical data places trust and authority to share that data on clinicians and hospitals. Studies [49] indicate that patients themselves place highest level of trust in doctors, hospitals and medical associations (see Figure 2.6).

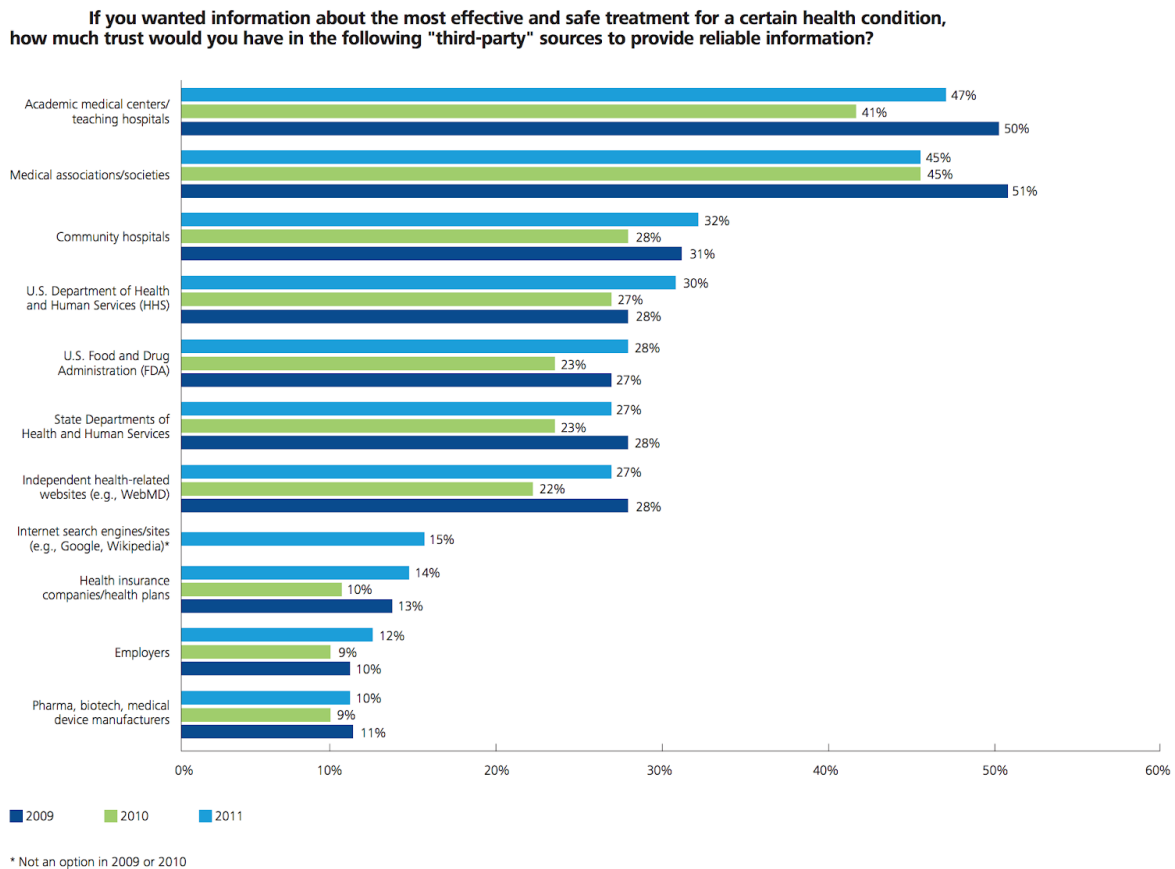


Figure 2.6: Who do patients trust? [49]

But as noted previously and detailed in Section 2.6 that medical data leaks is a widespread problem. Patients have very high level of concern about anonymity when sharing data for studies and 66% would consider switching clinician with more secure access to medical records [45][49]. As high as 80% of Americans are concerned about EHR privacy [50].

There are models that are being tried where patients have complete ownership of their data, sharing and monetization rights [41]. They choose the entities with whom their data is shared and

receive monetization outcomes. This serves to further research, keep patients informed and avoid data flowing into unknown entities without consent.

A more thorny data ownership question would be can patients select the data they want to divulge? Does the physician providing flu shots need to learn about heart condition?

Indeed, studies have glaring issues to highlight in this regard. They note that software vendors do not want to deal with added complexity of providing patients with explicit data sharing options. But given the choice patients does exercise this right frequently. Study done at *Regenstrief Institute at Indiana University* notes that 49% of the patients that participated withheld at least some information from their doctors [90]. Many patients have highlighted medical errors in their diagnosis and are concerned about future care and treatments based on that [91]. Without explicit ownership by patients, these issues cannot be addressed.

More and more people are collecting health data using various consumer devices to be better informed about their health. Usefulness of Personal Health Data (PHD) records for researchers can be seen in Figure 2.7, taken from [45]

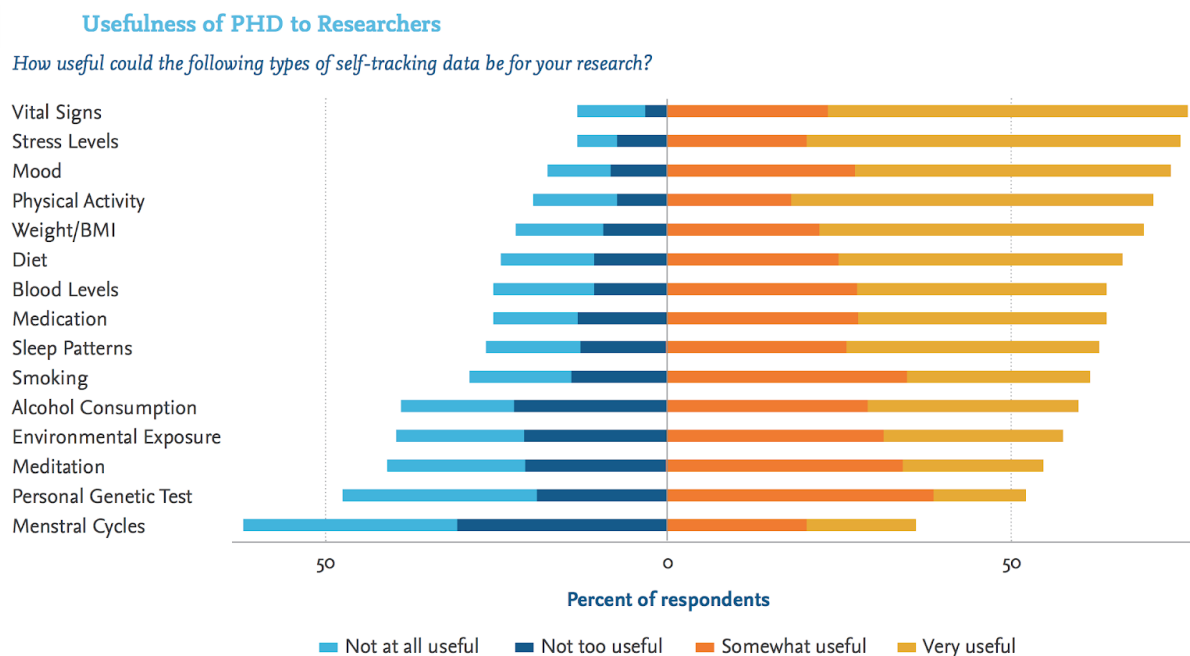


Figure 2.7: Usefulness of personal health records for researchers [45]

Many participants actively share their PHD records with their physician. With 54% of the respondents claiming in their understanding they own all of their data. Participants also expressed concerns regarding data sharing when done as Electronic Medical Record (EMR),

which as noted is lawfully not owned by them with 13% expressing aversion for sharing for commercial means.

2.3.3 Better Data Accessibility, Portability and Medical Care Choices

Following quote from an individual in study [45]

“I would like to own my data and whenever I go to consult with a professional and physician or a health care expert I’d like to be able to share that information with them and have them be privy to my entire health record history and I want to monitor it for problems and changes.”

Different roles in healthcare have varying access to patients data. And that access might not be available timely. With patients having access to their data and ability to grant access to clinicians when required, this can be mitigated. In one case, coroner has made demand for change in rules that stop NHS GPs in some areas ordering urgent Computed Tomography (CT) scans after an untimely death [80].

Medical data blocking is a serious concern and has been discussed at highest level of US government. The term “**information blocking**” is coined in *Report to Congress* in 2015 by *The Office of the National Coordinator for Health Information Technology (ONC)* [37]. The report notes that allegations continue to surface that some health care providers and health IT developers are interfering with the exchange or use of electronic health information in ways that frustrate the goals of the HITECH Act and undermine broader health care reforms. In addition, current economic incentives and characteristics of both health care and health IT markets create business incentives for some market participants to pursue and exercise **control over information in ways that significantly limit its availability and use.**

With patients as lawful owners and by giving them the ability to carry and share their data, situations like these can be avoided entirely.

Studies indicates that clinicians might be under pressure to prescribe certain medications for commercial pursuits [83]. With patients owning their data they may be able to cut down costs of medication drastically, may be able to use biosimilars or generics at a much lower cost [73]. Another study highlights issues with the social care system. It claims that no basic record exists between district nurses and GPs, social work and agencies. Because of this the study claims the system to be unsafe .[67].

These issues well can be addressed with patients being the source of truth for their medical data and by that being empowered to make more informed choices and be able to break data locks.

Any tools that enable patients to manage their health-care needs will be a game changer. - Dr. David Classen, Pascal's Chief Medical Information Officer

2014 data from Eurostat highlights that 1 in 3 deaths in Europe are untimely i.e. given the medical knowledge and technology they could have been avoided (Figure 2.8). Heart disease is identified as the primary category (32% attacks and 16% strokes) in preventable diseases [53]. Given the ubiquitous availability of consumer health devices, their data collection and availability of such data to patients as PHR, medical services should be able to create timely notification and address this issue. But data sharing concerns are noted in multiple jurisdictions and settings [37][54].

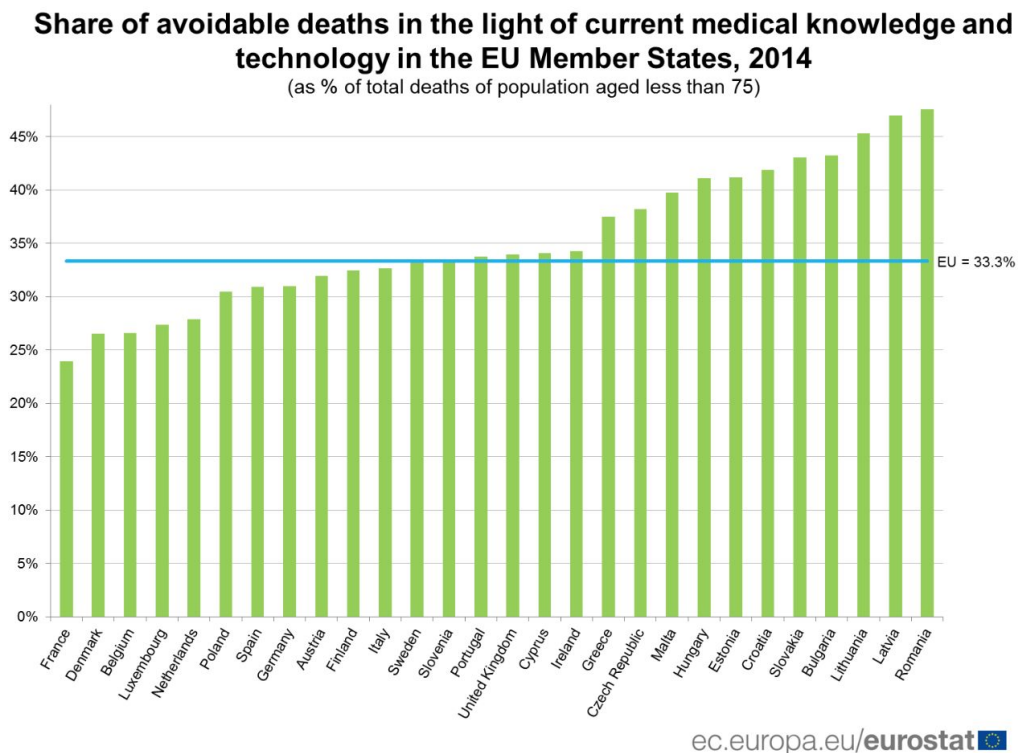


Figure 2.8 - Share of avoidable deaths in light of current medical knowledge and technology [53]

Medical errors are third leading cause of deaths in the US after heart attack and cancer. Numbers can be as high as 440000 a year [60][61]. Calling it death from medical care itself, calls for better reporting are made. Human errors and system failures are not noted despite calls being made to Centers for Disease Control and Prevention (CDC) for the same [62]. Apart from surgical complications; system breakdowns, judgement errors are cited as leading causes. To remedy this, hospitals are seeking increased usage of EMR systems and information technology. *But*

wouldn't patient carrying their data with them and having that data becoming available across different EHR systems alleviate these issues to some degree?

A leading benefit of EHRs is to provide audit trails of access of medical records in terms of the time, authorization and modification of medical data. HIPAA compliance requires EHR vendors to provide audit trail. But it is noted that although audit trails can provide hosts of benefits especially in medical malpractice cases, their admissibility is questionable. Sometimes users fails to log out, there are technical inconsistencies between vendors and even different patient identifiers [59]. *Patients having access to audit trails will lead to better transparency and standardization all around.*

Lastly, this section cannot be deemed completed without highlighting frailty of healthcare systems in wake of natural and manmade disasters. It is noted that crises do not respect geopolitical boundaries and health systems can undergo a sudden shock for e.g. a disease outbreak, earthquake, terror attacks, refugees [84][74]. It may sound far fetching but in a situation where population is displaced with original health institutions being under threat or overload. *With people owning their data either in mobile devices, cloud solution or some shared global infrastructure, there could be some alternatives be made available in difficult situations, where none exists.*

2.3.4 Conclusion

Patients in control of their data can alleviate many security and privacy issues, deter information blocking and increase choices for them.

Significant progress is made in healthcare systems in recent years due to them turning patient centric. Similar attitudinal shift towards patients' data ownership is required. Data ownership by patients can result in more engaged, informed and healthier population. It can also address hosts of accessibility, timely care and data standardization issues. With PHRs, their admissibility and consent based sharing, clinicians and researchers can benefit and provide better outcomes together with addressing hosts of privacy and security issues.

2.4 Challenges of Medical Data Ownership by Patients

Having noted hosts of benefits to patients, clinicians and healthcare system itself of medical data ownership by patients in the previous section, this section aims to identify known challenges towards that goal.

2.4.1 Technical

“We really need to drop interoperability as a competitive differentiator in this industry. Once everyone comes to the table and recognizes that we have a moral obligation to provide patients with their health records, I think we’re going to be much better off” - Zane Burke, president, Cerner Corporation

EHRs and various medical data cloud solutions that are in ubiquitous use and enable e-Health are complex software. They balance technical, legal and economic requirements. They enable hosts of clinical workflows and are integral part of model healthcare [77]. They may not be ideal but replacing them with a different technical solution on current level of integration posit a significant challenge.

There’s a level of data locking issues between different providers. They may be collecting different data and format of data that’s available to the patient may be different to what clinicians see [59]. This poses a challenge about data storage standardization. Until a common data elements for medical data is adopted system wide, most of the advantages of patient ownership in terms of accessibility and empowerment would remain elusive. Attempts for data standardization are in place as an open source, collaborative organization. [3][78].

A 2016 research study highlights that based on 10 million leaked passwords, 17% of passwords were “123456” [79]. There could be further challenges about technical literacy and affordability for any new technical solution across different population groups.

2.4.2 Societal

With equal reluctance to grant access on both sides, it becomes, as he notes, “not so much about ownership as it is about checks and balances.” - Anonymous in [88]

Many professionals asserts patients ownership of data [89] but as noted in other influential studies, data ownership is not same as property ownership. The advocacy group and thoughts against patient ownership of data highlights that potential for medical data for furthering research is substantial and ultimately beneficial for participants. It is ascertained that ownership isn’t the right question [44]. But this conclusion hides that government and commercial overreach is rampant in secondary usage of medical data. It is noted that sale of non-anonymized patient and provider data was carried out without patient consent or physician approval. Pressuring or coercing tactics for consent to data disclosure are also highlighted [63]. Even though a large number of medical professionals may be against the idea of patient data ownership and they may be coming from a good place, there seems to be glaring issues that aren’t being addressed adequately in current regime. As highlighted in Section 2.3.1, patients exercised selected sharing

of their medical records, given the choice. Multi method study carried out in UK on NHS patients highlights that some have concerns about being judged from their past ailments, especially the participants from socially disadvantaged or ethnic minority backgrounds [91].

I know it could lead to negative labelling, definitely. And it just comes down to the human level, with the nurse, the GP dealing with patients, how it will affect their treatment of people, I'm sure it will have an influence on that. There will be someone down the line that will react negatively, there's no doubt about it. - Anonymous in [91]

Racial data is not only collected for patients but for clinicians as well. It is used through law and policy enforcement in healthcare settings. Following is a quote from NHS GP [94]

*“Not even a letter from Theresa May is enough to **protect me and my patients** from racial profiling and everyday **microaggressions that these policies encourage**. Infecting the NHS with immigration policies clashes with the standards of care” - Roghieh Dehghan, part time GP in north London, NIHR in-practice fellow at the Institute of Global Health at University College London*

Another social challenge with patients ownership of data in the other direction could be overreliance on virtual communities and remote/mobile health. This may provide hosts of benefits in terms of 24/7 always on care but it could lead to reduced doctor-patient interaction and engagement [76].

2.4.3 Economical

In a recent incident a service ‘GP at Hand’ was launched in west London as a pilot by a group of GPs and a private healthcare company. It allows patients to receive ‘virtual’ consultations on their smartphones over video link. Group of GPs expressed concerns about loss of income they may incur if patients switch to such services. Some calling the service ‘morally questionable’ as it may not be accessible to all income groups. [95][96]

“Financial incentives are rotten to the core” - Margaret McCartney, general practitioner

There are hosts of reports mentioning overprescribing and misaligned prescribing to serve invisible commercial interests. It is highlighted that overpriced drugs are prescribed when cheaper versions or generics are available. Conflict of interest with wellness of patients and hitting sales targets is noted [83]. Clearly the current climate treats patients as a natural resource to drive value from instead from of creating an inclination to serve them. Does this place today’s physician’s in violation of Hippocratic Oath [105]. It should be noted that World Health Assembly recognize the need to improve access, affordability and quality of generics [73]. Medical Tourism is a growing industry worldwide with millions of people taking advantage of better to similar care

for cost benefits. Patients can benefit immensely and have an impact towards unreasonable medical costs in their country of origin if their medical data is owned fully by them [106].

Lastly, patient activation, which refers to their ability to manage their health varies considerably. In US, less than half of the adult population is at high level of activation. It is noted that activation levels are considerably low for people with low incomes, less education, Medicaid enrollees, and people with poor self-reported health [48].

2.4.4 Legal

The text '*Much Ado About Data Ownership*' by *Barbara J. Evans* [42] has been cited by multiple sources that have discussed data ownership by patients and identified legal climate as one of the factors towards it. The text claims that patients will not gain much as HIPAA and HIPAA Final Rule provide them with protections i.e. sought by ownership. [89]

The framework of patient entitlements and protections afforded by the HIPAA Privacy Rule and the Common Rule is strikingly similar to what patients would enjoy if they owned their data. - Barbara J. Evans, Professor; Co-director, Health Law & Policy Institute; Director, Center for Biotechnology & Law, University of Houston Law Center

As noted earlier in Section 2.2.4.1 that HIPAA is not about medical data ownership and medical data laws do not assign ownership to patients. The claim that patients will not gain because of legislation change does not hold merit.

Medical entities do misuse their authority granted to them under law. They continuously put commercial pursuits first. And unknown human biases in clinicians and other medical staff does put patient safety at risk. Unjust discrimination and ethical issues were noted against overreach of Mental Health Act [98].

2.4.5 Conclusion

There are multiple interests at play. And reaching to a consensus for a new paradigm is a significant challenge. Not only monetary but cultural and time investments are made with different factions holding varying incentives.

A disconnect between medical fraternity's understanding of data ownership and patients' legitimate concerns should be noted. Evidence of unauthorized data sharing for commercial pursuits is worth highlighting.

Legal definition not considering patients as owners remain a significant challenge.

2.5 Solutions for Medical Data Ownership by Patients

“We must strike a balance between data ownership, interoperability, security, and dynamic consent for patients, so that data can be used and shared at the right times and under the right circumstances” - Jim Nasr, chief software architect for the Centers for Disease Control and Prevention (CDC)

2.5.1 Open Data

Care.data initiative by NHS, a platform that intended to enable individual data sharing with researchers and businesses was scrapped in 2016. Lack of public information and poor implementation of checks and balances. Caldicott Principles [20], first published in 1997 was updated in 2016 following the controversy with focus on security, consent and opt-outs [118]

But it is noted in [72] that a group of citizens continue to share data with medtech companies using wearables. Paper notes there could be a group of citizens who consider their medical data as **donated**. Health coop initiatives are on the rise where people can bring their medical data from multiple sources and have transparency and control on deciding with whom this data should be shared [41].

2.5.2 Cryptographic Control

Paper [99] highlights hosts of benefits in using blockchain based solution for medical record management. Patient managed health care records, immutable audit trails, increased safety of records etc are listed as advantages of such a system. Related projects and papers in this space are also listed.

But two recent projects Linnia [100] and Solid [82] are making serious attempts in solving data ownership from bottom up. Solid is a project by *Tim Berners-Lee, inventor of World Wide Web*.

Solid's Github page [119] define Solid as proposed set of conventions and tools for building decentralized Web applications based on Linked Data principles. Solid is modular and extensible. It relies as much as possible on existing W3C standards and protocols. About Solid section goes in further details but in essence this project aims to provide capabilities like identity, authentication and login, authorization and permission lists, contact management, messaging and notifications etc. in a decentralized manner. By **decoupling content from the application and providing users choice** about where to store the data and allowing who can access it.

Linnia is also an ambitious and resourceful project. It imagines the web 3.0 (current is web 2.0) as being able to provide data self-sovereignty to users by leveraging Interplanetary File System (IPFS), blockchain based identity and being able to control access to data with other identities. Linnia aims to solve the last part by being a data protocol built over Ethereum [120].

2.5.3 Law Changes

Better governance for health can be achieved through appropriate public health legislation [75]

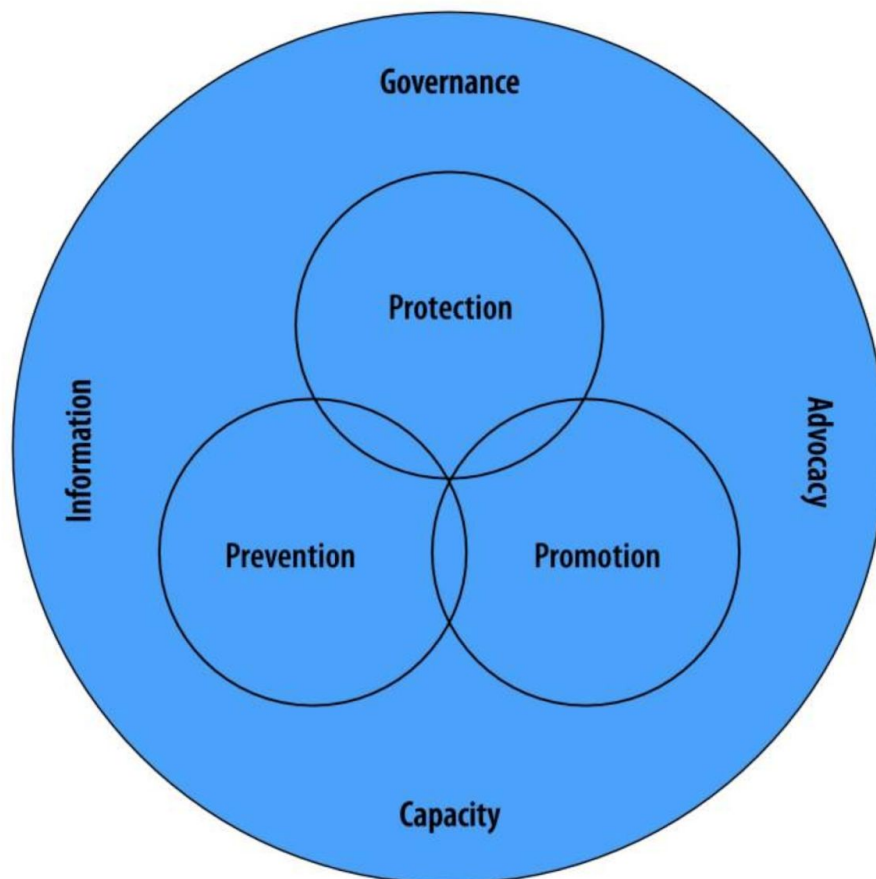


Figure 2.9: Core services are protection, prevention and promotion. Enabler functions are information, capacity, advocacy and governance [75]

Number of sweeping changes are delivered in HIPAA Omnibus Final Rule [51]. With law calling for strengthening the limitations on the use and disclosure of protected health information for marketing and fundraising purposes, and **prohibit the sale of protected health information without individual authorization.**

Indeed, patients becoming lawful owners of their medical data would deter incidences like information blocking, implied consent and lack of opt-outs straightaway.

2.5.4 Conclusion

Open data initiatives are being created to address some data sharing concerns. These platforms yield data sharing control to patients. It is interesting to note the altruistic nature of data sharing by patients. Many technical solutions are in the making that separate data from applications and allows control of building access relationships on data owners. But they are years away from public use and are shrouded in unknown obstacles. Legal amendments seem like a best foot forward to trigger wider discussion in area of medical data ownership by patients.

2.6 Medical Data Leaks, A Widespread Problem

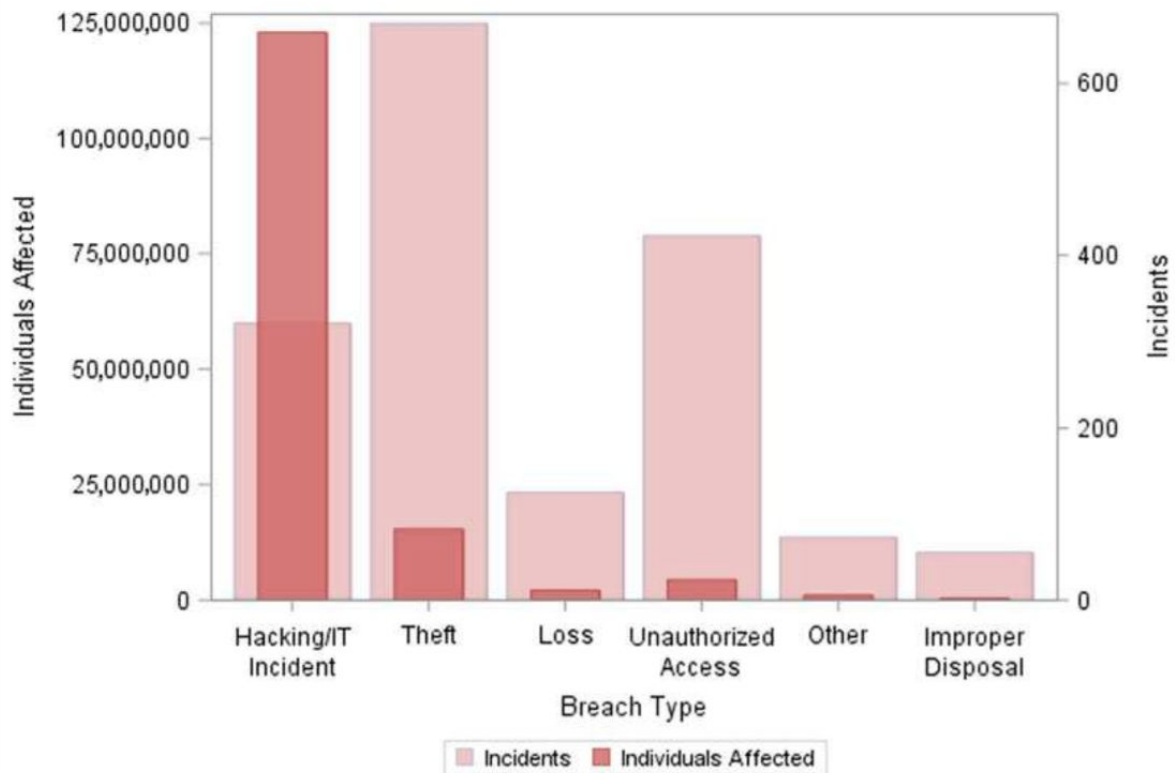
Medical data leaks is a widespread issue [21]. It causes social and personal harm and reduces trust in the institutions [22][23]. It may seem that creating more checks and balances would hinder data availability for research but not doing so also prevents us from reaching to optimal use of such data[24].

Over 173M Americans have their data leaked in 2008. Data obtained from Office of Civil Right [26] includes following reasons

1. Hacking/IT Incident
2. Theft
3. Loss
4. Unauthorized Access
5. Other
6. Improper Disposal

Following Figure 2.10 is obtained from [26]

Figure 2. Types of Privacy Breach Incidents and the Number of Patients Affected by Them Among Covered Entities^a
 [Color figure can be viewed at wileyonlinelibrary.com]



^aData derived from authors' analysis of Office for Civil Rights data on breach incidents between October 2009 and August 2017. Incidents described as "Unknown," "Other," or that were missing a description were grouped under the "Other" category. Where the type of an incident was categorized in more than one group by OCR, the incident was assigned to the primary group. For example, an incident OCR described as "Theft/Loss" was categorized under "Theft."

Figure 2.10: Types of privacy breach incidents and number of patients affected by them [26]

The figure shows number of incidents in each category and also the individuals affected. It is interesting to note that number of **data theft** and **unauthorized access** incidences are far higher than **Hacking/IT**. Indeed, 41% of data leaks and breaches happens due to insiders [27].

Data leaks are indeed rampant [28]. But protection of medical data becomes much more crucial. Some of the known medical data leaks have lead to following [29].

1. Identity theft
2. Insurance premiums going up
3. Employment discrimination

Indeed many people have opted out from medical research due to rise in data breaches [34]

In UK, almost half of data breaches (43%) have been related to health sector in 2014-2016. The study [10], also notes the increase in number of such incidences. Although at surface it seems like, this is caused by the known WannaCry incident [31]. Study notes

Critically, the findings showed that the many of these incidents are attributed to human error, rather than external threat.

In another incident in UK, 150000 people were affected in a software error, where the option to opt in for **secondary usage** of data was made unavailable. In 2017, 26M people were affected in UK in a major breach where 1 in 3 GP clinics were affected and made this data available to thousands of strangers [33]

Secondary usage of medical data and such authorization is a known cause of data leaks [35].

In 2018, Health South-East RHF, the organization that manages Norway's hospitals disclosed that half of Norway's population's medical data was leaked [36]. The attack is classified to be done by 'advanced' or 'professional' hackers.

2.7 Data Ownership Studies

An empirical study titled "A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy" [2] notes that consumers often want more choices than what's available. It is noted that over 80% of participants have disclosed information at some point online which they wish they didn't had to. Low level of trust in government as data collector and keeper is highlighted. Call for empowering users and giving them more control over their data is made. For a long term solution rethinking of existing data privacy laws is proposed. Although the study

sought to increase consumer engagement in online marketplaces, parallels can be drawn with patients and hospital systems.

2.8 Conclusion

Data ownership is a complex issue encompassing education, awareness, social, economical, technical and legal spheres. Legally accepted definition of medical data ownership seems to be preventing a required wider debate for ownership by patients.

The wider, non obvious benefits of patient empowerment shouldn't be ignored. Medical data is extremely valuable on monetary level. There are both commercial and social issues associated with its unfair usage and sharing. Patients view data sharing with altruistic intentions. Given the choice, patients do exert more control over data. Commercial exploitation of patient data with implied consent is an issue that needs wider discussion. Similarly role of external entities needs to be better defined on policy level.

Without proper education and training to use any new solution, security and privacy issues may worsen. Any solution must be designed in a way that can be used by a wide demographic, seperated by age, education and financial reach.

Even as I write this conclusion. GlaxoSmithKline, a pharmaceutical giant has made investments in 23andMe, a genome sequencing company highlighted in [Section 2.2.2] and GSK will have access to latter's customer data, **who have consented for data sharing for furthering research**. Concerns about the role of external entities were highlighted in Section 2.2.1.

What would likelihood of these mergers be if data ownership was with the patients and they were to selectively opt-in and were able to request deletion of previously shared data from any secondary usage?

As a 23andMe customer myself, this is really strange definition. 23AndMe assumes goodwill of Google, who has the **highest** brand value [102]. While GSK is not viewed in similar light with having paid over \$2B in litigation in last 10 years [103]. This story has been discussed online on Twitter, Reddit and Hacker News, with consumers asking for transparency, expressing shock and distrust. Following screenshots capture some of the comments. Hacker News is a reputed forum to discuss tech related news and development. Some commentators also noted that cost of 23andMe kits have gone down considerably in recent months and this is something that they were anticipating. [65][66][86][103][104].

Figure 2.11 below highlights the tweet by 23andMe's CEO announcing the above investment. Figure 2.12 and Figure 2.13 shows top social media comments in response to this announcement.



Anne Wojcicki ✓

@annewoj23

Follow



Thrilled to announce our collaboration with [@GSK](#) to accelerate our ability to make novel treatments a reality. Our customers don't want to wait for solutions to appear; they want to actively participate. With GSK, we can to make breakthroughs even faster!



A Note On 23andMe's New Collaboration with GSK - 23and...

23andMe announces the launch of a collaboration with GlaxoSmithKline (GSK) to accelerate our ability to make meaningful discoveries in therapeutics to treat disease.

blog.23andme.com

Figure 2.11: Screenshot of tweet by Anne Wojcicki, CEO, 23andMe; announcing GSK investment

CEO and Co-Founder of 23andMe tweets about GSK investment in above tweet. Following are top comments (votes, retweets) on this



Privacy Matters @PrivacyMatters · Jul 26



Replying to [@annewoj23](#) [@GSK](#)

Under the GDPR, health related and genetic data are special categories of personal data that attract quite strict rules .. such as requiring explicit consent (or another strict condition 🤔). Might I ask what condition under Article 9 of the GDPR that 23andMe is relying on here?



Patrick Karlsson ⚡ @Patrickesque · Jul 25

Replying to @annewoj23 @GSK

Making money off our genetic data?

I just revoked all permissions/consent for my 23andme results. See ya



19



71



466



Figure 2.12: Screenshots of most popular responses to Anne Wojcicki's tweet (figure 2.11)

Top Hacker News comments on this story.

▲ dayvid 3 days ago [-]

I asked 23andMe if there was any way to delete my genetic data from their site after the Equifax hack news. From their response:

"23andMe and our third party genotyping laboratory will retain Genetic Information, date of birth, and sex as required for compliance with applicable legal obligations, including the U.S. Federal Clinical Laboratory Improvement Amendments of 1988 (CLIA), California Business and Professional Code Section 1265, and College of American Pathologists (CAP) accreditation requirements.

23andMe will also retain limited information related to your account and data deletion request, including but not limited to, your email address, account deletion request identifier, and record of legal agreements for a limited period of time as required by contractual obligations, and/or as necessary for the establishment, exercise or defense of legal claims and for audit and compliance purposes.

We recommend that you review our full Privacy Statement for more information about deleting your data before submitting your request."

So basically, once your in their system, you can't get out.

And you're paying them money for this.

Any way to do self-DNA testing?

▲ TrainedMonkey 3 days ago [-]

Make no mistake about what is happening here. GSK is buying access to all of the genetic data that 23andMe has. This is why I am wary to use any 23andMe type of service.

"The partners plan to use 23andMe's data to jointly discover drug targets."

They will claim all kinds of protections of course, but it is only a matter of time until genetic data starts being resold.

Figure 2.13: Screenshots of top Hacker News comments on GSK's investment in 23andMe

I received email from 23andMe after the announcement and have asked them about a separate opt out for GSK data sharing (Figure 2.15). I never received a response. Following (Figure 2.14) is the information from their consent form, which makes the action to withdraw consent now worthless. **This should not have been the case.** And there should be more transparency and dialogue on such arrangements.

Can I stop taking part in 23andMe Research?

- Yes, you can withdraw from 23andMe Research at any time. Any of your data that have already been entered into a study cannot be withdrawn, but your data will not be included in studies that start more than 30 days after you withdraw (it may take up to 30 days to withdraw your information after you withdraw your consent).

Figure 2.14: Answer to the question “can I stop taking part in 23andMe Research?” in 23andMe consent form

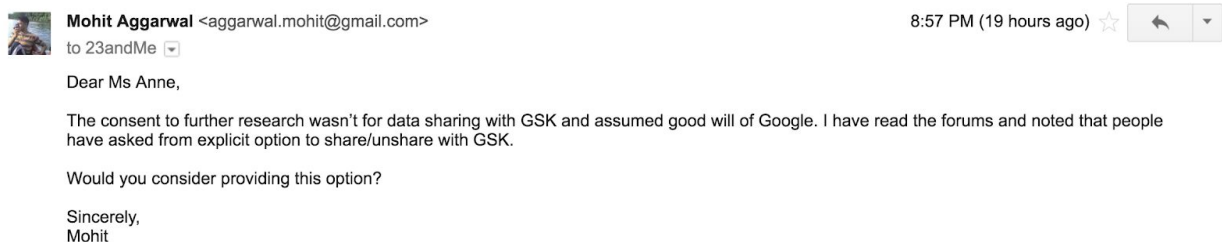


Figure 2.15: Screenshot of researcher's (a customer) query to 23andMe for explicit opt-out option

In another development related to genetic data, Canada is using it for deportations [87]. The risks associated with sharing of such data are not well understood and a demand for patient education together with legislation revisions should be made.

Medical services are largely understood to be government lead with lots of UN initiatives and national programmes. But they are indeed an amalgamation of private interests and public policies. We have learned that more ethical businesses are good for the economy [101]. As that demand intensifies on them, medical and other perceived public domain entities should be brought under a similar scanner.

I tried to be impartial in the literature review but that cannot rule out the possibility of unconscious bias in favor of patients as I identify as a person with that group. To resolve this and to get a better picture it is equally important to speak with diverse group of medical professionals as it is to a diverse group of patients.

3. Research Methodology

3.1 Introduction

Aim of this study is to understand the complexities around data ownership in medical systems and services. Study aims to identify understanding of general public (patients, consumers, end users) and medical professionals around medical data ownership, concerns and understanding around data leaks, data privacy laws and to further identify solutions in this regard.

This section highlights overview of methodology used for the study. It includes rationale for selection of this methodology, researcher's positionality, development of interview protocol, selection of questions, overview of study participants, their selection and corresponding ethical and data analysis paradigms.

3.2 Study Type and Rationale

As learned from section 2, medical data ownership is a multifaceted problem that encompasses multiple policy, social and economic spheres. Purpose of this research is to gain wider understanding of this topic from multiple perspective. Where there's no right and wrong answer but subjective responses can help uncover the patterns, experiences and expectations from the participants. Towards that cause qualitative method of research was found to be best suited. Interviews were conducted in semi structured fashion to explore implications, challenges and solutions for medical data ownership by patients.

Positionality and avoiding bias becomes an important factor in such a study. Section 3.3 and 3.4 details researcher's positionality and steps taken for avoiding bias for all involved.

3.3 Researcher's Positionality

Researcher has technical background and was aware of some technical solutions under development towards allowing patients full control over their medical data. Initial plan was to search through literature, learn about existing solutions and then propose a technical solution based on available knowledge and best practices.

But initial and detailed literature search quickly highlighted that this is a wider issue. And a technical solution will not solve it without taking into account other factors.

Researcher also identifies with the patient camp and is aware of underneath bias of giving patients more control over their data in wake of multitude of leaks and other available statistics.

3.4 Avoiding Bias

Following steps were taken to avoid any bias

1. Initial plan was to speak with as many patients as possible. But it became apparent that medical professionals should be included in the study as a separate group and should have similar but different set of questions
2. To avoid the bias towards known or personally favorable solutions and to expand knowledge, a question is included for each participant group about how would they design a system where medical data ownership lies with the patients
3. A diversity within each group was deliberately sought by approaching participants with varying socio-economic-educational-role background
4. For literature review, counter views towards medical data ownership were sought and cited.
5. Lastly, to avoid participant's bias original title of the study was hidden from them and more generic 'Medical Data Ownership' was given to them as title of Information Sheet and Consent Form (Section Appendices F and G respectively)

3.5 Methodology and Plan

Literature and existing studies are cited for identifying the challenges and proposed solutions towards data ownership. Need for interviewing patients and medical professionals arises to understand social, user and system frictions towards this goal.

It is worth highlighting again that term patient here is used as an inclusive term. Any end user of medical services is considered worthy of input for the purpose of this study. As they can provide insights based on their past experiences and their understanding of pain points of others

Based on literature review questions for patients and medical professionals are identified. For patients questions related to medical data ownership, awareness of data leaks, general privacy awareness and concerns and views regarding medical data sharing were identified. For medical

professionals similar but more concise mirror questions were identified. Following sections details these questions and their rationale in detail

Before the beginning of primary interview questions, a placeholder question is asked to patients “When did you last visited a doctor?” This is simply to draw participant’s attention towards medical domain. No such question is posed to medical professionals

Some follow up questions that are not listed here are asked leveraging on the semi structured nature of this study. For e.g. what is the meaning of medical data ownership for you? Or Would patients highlight their conditions to you? Etc. These are highlighted in in greater detail in section 4.3

3.5.1 Questions for Patients

Following are the questions for patients. Table 3.1 details rationale for each of them

No.	Question	Rationale for Inclusion
1.	Can be please share a. Your occupation and highest education level attained? b. Can you describe what responsibilities you have on everyday basis?	These questions are to be able to understand and cite difference in participant responses based on diversity in their background
2.	In your understanding who owns your medical data?	To understand who does general public consider as medical data owner. At this stage also the detail about what is meant by medical data ownership can be given. Literature review identifies that legally patients are not considered medical data owners. But do they know that
3.	If you visit a medical professional or facility for an injury or consultation, in your understanding for how long is your medical data related to this retained?	To understand patients understanding of data retention times. It is learned from literature review that In some jurisdictions data is required to be kept for certain number of years, does patients have similar understanding
4.	Are you aware of medical data leaks and breaches?	To understand if they know medical data is routinely targeted. As highlighted in literature review and Introduction

		section, medical data leaks is a widespread problem in size and frequency. Does general public know this.
5.	How do you think your medical data can be misused? (Follow up questions may prompt respondents to consider: c. Identity theft d. Insurance premium going up e. Discrimination)	It is learned that there are known repercussions of medical data leaks towards patients. Do they understand these
6.	If you were to have complete ownership of your medical data in terms of a. Authorizing and limiting access b. Being able to revoke access c. Knowing the time of data usage and modifications What advantages and disadvantages would you perceive for you as a patient?	
7.	Are you aware of any data privacy laws? Were you before GDPR?	This is to understand general societal awareness about data privacy
8.	Your medical data is scattered across services medical devices, consumer devices (apple, fitbit etc), medical and insurance companies and entities. Would you prefer to have some control over secondary usage of this data?	To understand if patients realize that they are generating and sharing medical data when they use these services. Further do they understand their data can be shared with third parties and if they would like to have control over this participation
9.	Some of the medical data is used to further research and studies. Would you like to have some control over how their outcomes are monetized?	It is learned through literature review that patients are interested in data sharing to further research but have concerns regarding commercial means towards this. This question aims to understand their positioning regarding commercialization
10.	Final question, if you were to design or implement a system where data ownership	This question serves dual purpose. Apart from opening a window in terms of

	is transferred to you. How would you do this? What are patients' responsibilities and rights. What are the system constraints etc?	learning about potential new solutions about medical data ownership. It also highlights engagement and inclination of general public towards this.
--	--	--

Table 3.1 - Questions for Patients and Rationale for inclusion

3.5.2 Questions for Medical Professionals

Following are questions for medical professionals. Table 3.2 details rationale for each of them

No.	Question	Rationale for Inclusion
1.	Can you please state 1. Your role and expertise 2. Highest education level attained 3. Your primary responsibilities on everyday basis	These questions are to be able to understand and cite difference in participant responses based on diversity in their background
2.	In your understanding who owns medical data?	While the question for patients ask the question as "your medical data". This question asks medical professionals who owns medical data. This is to understand the contrast between two groups. Do they have similar understanding
3.	Are you aware of medical data leaks and breaches?	As medical professionals, it is expected that this group of participants will be more aware of medical data leaks. This is again to highlight and understand the contrast
4.	Are existing data protocols in place sufficient to prevent data breaches? What changes should be made in your understanding in these protocols to strengthen them?	If participant is sufficiently aware about medical data leaks, this question can help gain understanding from their experience, if they identify certain changes to better the system
5.	Are you aware of data privacy laws? Were you before GDPR?	To gain understanding of participant's prior understanding any data privacy laws.

6.	Do you have any concerns regarding patients having control over their medical data?	This is an important question to ask medical professionals. It can help understand effect and interference of patient data ownership on their everyday practice, requirements and duties
7.	Final question, if you were to design or implement a system where data ownership lies with patients. How would you do this? What are patients' responsibilities and rights? What are the system constraints etc?	This is an exploratory question to ask about a solution. If during the interview, participant is perceived to be against patient ownership of medical data, this question is not asked

Table 3.2 - Questions for Medical Professionals and Rationale for inclusion

All these questions stand on their own merit and can be valuable towards the research question and gaining insights for further research. Table 3.3 below lists similar questions asked in both groups. These can help identify general differences in opinion, understanding and professional constraints. These questions are can highlight alignment and lack thereof between two groups.

Question regarding system design is excluded from this list as it's not always asked.

No.	Question for Patients	Question for Medical Professionals
1.	In your understanding who owns your medical data?	In your understanding who owns medical data?
2.	Are you aware of medical data leaks and breaches?	Are you aware of medical data leaks and breaches?
3.	Are you aware of any data privacy laws? Were you before GDPR?	Are you aware of any data privacy laws? Were you before GDPR?

Table 3.3 - Common questions in both groups

Research aims to produce some data visualizations based on clustering of respondents. For e.g. response to having prior information about privacy law based on country of origin, age, highest level of education etc.

3.6 Research Participants

Diversity in socio, economic and educational background in user participants and in roles and responsibilities of medical professionals is crucial for this study. Towards this goal people from varying backgrounds were approached. From work, friend circles and fellow students. They were encouraged to direct more people towards this study in their contacts

Under no circumstances were these people under any obligation to share information or participate in the interview. It is to highlight that this work was not conducted in any professional capacity. People approached at workplace did not had any direct work relationship with the researcher.

Some NGO workers are also known to the researcher and they were approached as well.


Some medical professionals are known to the researcher. They were approached in their capacity of being an expert and were encouraged to direct more people towards this study.

This is a qualitative study. Original goal was to approach 15 people in each category. 10 people were interviewed in **Patients** category and 6 in **Medical Professionals**. Section 4.1 give some details about the participants' background

1. **Patients/General Public:** A mix of backgrounds is crucial for this study. Three groups of people are known to the researcher. Professional contacts (no direct working relationship), out of work contacts, NGO contacts. Mix of people from each group were included and diversity in backgrounds (country of origin, sex, age etc) was sought
2. **Medical Professionals:** Towards the study's purpose it is important to speak with medical professionals with different areas of expertise and experience. These professionals are known to the researcher as work contacts (no working relationship), fellow students and friends.

3.7 Data Collection and Analysis

Semi structured and exploratory interviews with participants was recorded by the researcher on an iPhone smartphone and was transferred to a secure Dropbox folder. Contents were only accessible to the researcher and their supervisor and were not be shared with any third party. Participants were informed that this recording belongs to them entirely and they can request deletion of their recording anytime until the publication.



Participants will be identified using a **participant code** generated using combination of their initials, occupation, group, company etc. For e.g. MA-CRM (Name - Company Name), TA-VE (Name - Group), YW-ST-EMB (Name - Education - Expertise)

Most participants are known to the researcher and directly contactable through existing email and social media links. Some participants share the same groups as the researcher and joined the study on announcement in the group. Participants were approached using electronic mediums

1. Email
2. Messengers (MS Teams, Skype, Whatsapp etc)
3. Social media contacts (Facebook, LinkedIn)

They were given a high level overview about the research and asked for a time and place for interview at their convenience if they like to participate. During the interview participants were told on tape that they can retract anytime if they desire before the publication of this work


Participant identities are anonymized but for the purpose of the study their role, occupation and education level is used during Results and Discussion (section 4 and 5 respectively). Under no circumstances this information will lead to personally identifiable information of the participant.

Their recorded responses were disseminated by the researcher to understand the concerns raised, to draw conclusions in terms of patterns and to further identify areas to focus for the purpose of the study

The Information Sheet (Appendix F) avoids being too explicit about the exact topic of the study as there's a chance that participants get biased and start making their answers with data ownership as they like it to be. They were be asked questions as detailed in section 3.5 regarding and at the end were told about complete nature of the study.

3.8 Ethical Considerations

The researcher will ensure that participants in the study are fully informed about the research topic by providing them with background information. Their participation will be entirely voluntary and information about revoking permission to their contributions at any point will be clearly shared with them before data collection begins. The researcher will only recruit participants who are capable of giving informed consent. There will be no attempt to mislead participants as the purpose of the study is to gain an understanding of the patient and clinicians experience of the topic at hand. Data collected will be stored securely and anonymised, as described above. The



anonymised, unaggregated data will not be shared with third parties, except the project supervisor. The researcher will inform participants at the end of the interview about the process that the information will be put through as part of the study. They will also be advised that they are welcome to a copy of the study and findings once they are complete.

4. Results

“I don’t know what the legal retention policy is but there are doctors that have kept the records for a long long long time” - Study Participant

“I haven’t heard of medical data leaks but about credit cards” - Study Participant

“I don’t agree about sharing my medical data if someone is making money off it. But I agree straight away if it’s for greater good” - Study Participant

“It’s a money driven industry” - Study Participant

4.1 Participants Background

For the purpose of data collection (section 3.7), participants code was started with their initials. That information is not relevant. For the results they will be cited as P-A/B/C For patients group and MP-A/B/C For medical professionals group.

Table 4.1 below provides broad overview of patient participants background and Table 4.2 of medical professionals. For patients, their **country of origin** is provided and for medical professionals their **country of practice** as that would be more relevant. Section 4.1.3 give details regarding **education** and **professional levels**.

These indicators are important in understanding different attitudes, engagement levels, concerns and inclination for adopting a different system

4.1.1 Patients Group

No.	Code	Country of Origin	Educational Level	Professional Level
1.	P-A	France	High	High
2.	P-B	Ireland	Medium	Beginner
3.	P-C	United States	Medium	Beginner
4.	P-D	Ireland	Medium	Medium
5.	P-E	Ireland	Medium	High

6.	P-F	United States	High	High
7.	P-G	Ireland	Low	Beginner
8.	P-H	Croatia	Medium	Medium
9.	P-I	Ireland	Medium	Medium
10.	P-J	Austria	High	Beginner

Table 4.1 - List of patient participants, their code and some background indicators

4.1.2 Medical Professionals Group

No.	Code	Country of Practice	Educational Level	Professional Level
1.	MP-A	Ireland	Medium	Medium
2.	MP-B	Ireland	High	Expert
3.	MP-C	United States	Medium	Expert
4.	MP-D	Ireland	Medium	Expert
5.	MP-E	Poland	Beginner	Beginner
6.	MP-F	Ireland	Medium	Medium

Table 4.2 - List of medical professional participants, their code and some background indicators

4.1.3 Participant Attributes

Participants' exact title or expertise are omitted in these tables. Some quotes refer to their expertise without referring to their code to avoid any possible identification

Education and Professional Levels are broad indicators. Table 4.3 give details regarding those

Education Level	Low	Undergrad or below
	Medium	Finished Bachelors or Masters
	High	Finished/Pursuing PhD

Professional Level	<table border="1"> <tr> <td>Beginner</td> <td>Intern</td> </tr> <tr> <td>Medium</td> <td>Early Career</td> </tr> <tr> <td>Expert</td> <td>Long Career</td> </tr> </table>	Beginner	Intern	Medium	Early Career	Expert	Long Career
	Beginner	Intern					
	Medium	Early Career					
Expert	Long Career						

Table 4.3 - Details about education and professional level indicators

4.2 Contrasting Questions

Table 3.3 lists some similar questions for each group. This section highlights the responses to underscore the overlap and disconnect between patients and medical professionals

4.2.1 Medical Data Ownership

Table 4.4 lists the raw responses by each participant towards the question regarding medical data ownership. Participant group can be deduced from their code. Column deduction classifies these responses and Rationale lists reason for this classification

Code	Medical Data Ownership	Deduction	Rationale
P-A	<i>Multiple Entities, should ideally be me</i>	Clinicians, Hospitals	Participant would like to own their data but understand that this is not the case
P-B	<i>Myself and whoever has it, Talks about equal control</i>	Patients, Clinicians, Hospitals	Participant considers themselves as owner but also consider any entity who have their data as owners. This sentiment comes from the understanding of these entities using the data for providing care
P-C	<i>I own it, medical professionals can use it,</i>	Patients	Participant is aware of data ownership to a degree

	<i>talks about control</i>		
P-D	<i>Me, retained by others, can disclose if its best interest to help me or others</i>	Patients	Participant consider themselves as owner but is okay to share that data for care and research
P-E	<i>I own it, they are controllers</i>	Patients	Participant strongly consider themselves as owner
P-F	<i>Myself as it's data about me</i>	Patients	Participant strongly consider themselves as owner
P-G	<i>HSE</i>	Government	Participant considers a government department to be the owner of their medical data
P-H	<i>Hospital</i>	Hospitals	
P-I	<i>GP</i>	Clinicians	
P-J	<i>I own it, some parties have access</i>	Patients	Participant identifies themselves as owner and consider data is shared with other parties
MP-A	<i>Hospitals</i>	Hospitals	
MP-B	<i>The clinic, patient as well probably</i>	Hospitals	Participant strongly consider medical entity that employs them as owner. But they mention that patients have some of this data
MP-C	<i>Hopefully patients, in real world I don't know</i>	Hospitals, Clinicians, External Entities	Participant has strong medical background as a professional. They do not consider patients as owners
MP-D	<i>Clinicians, Hospitals, Patients should have access</i>	Hospitals, Clinicians	Participant considers clinicians and hospitals as owners but mentions that patients should have access
MP-E	<i>Patients owns it, doctors have access</i>	Patients, Clinicians	Participant strongly considers patients as owners with doctors having access to their

			data
MP-F	<i>Information that Patients share, healthcare entity should be able to use it in anyway for their care</i>	Patients, Hospitals	As long as healthcare entity is making use of the data for patients care they can be considered as owners as well

Table 4.4 - Responses about medical data ownership

These responses can easily be mapped to data producers and processors identified in section 2.2.1. Chart 4.1, 4.2, 4.3 and 4.4 below plots the above data. Chart 4.2 is simplified version of patients responses where their ownership identification is shown as patients vs others. Chart 4.3 shows the data owners choices from medical professionals and Chart 4.4 shows simplified version of that with patient vs non others. It should be noted that if a participant has responded with patients and some other choice, their choice is counted in both categories

Medical Data Owners As Per Patients

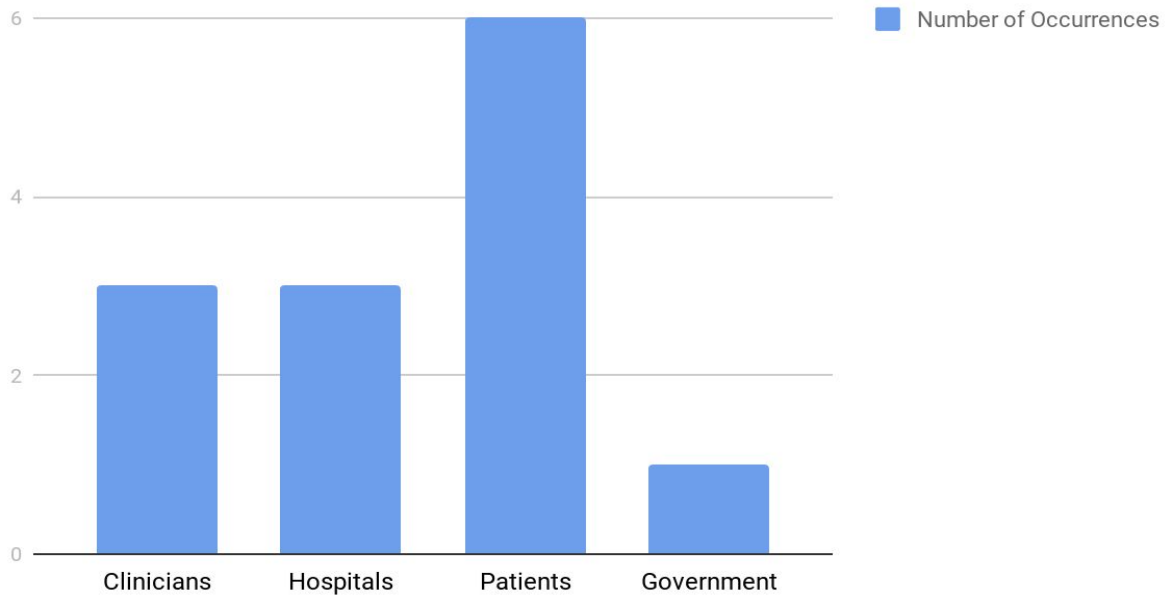


Chart 4.1 - Medical data owners as identified by patients

Medical Data Owners As Per Patients (Simplified)

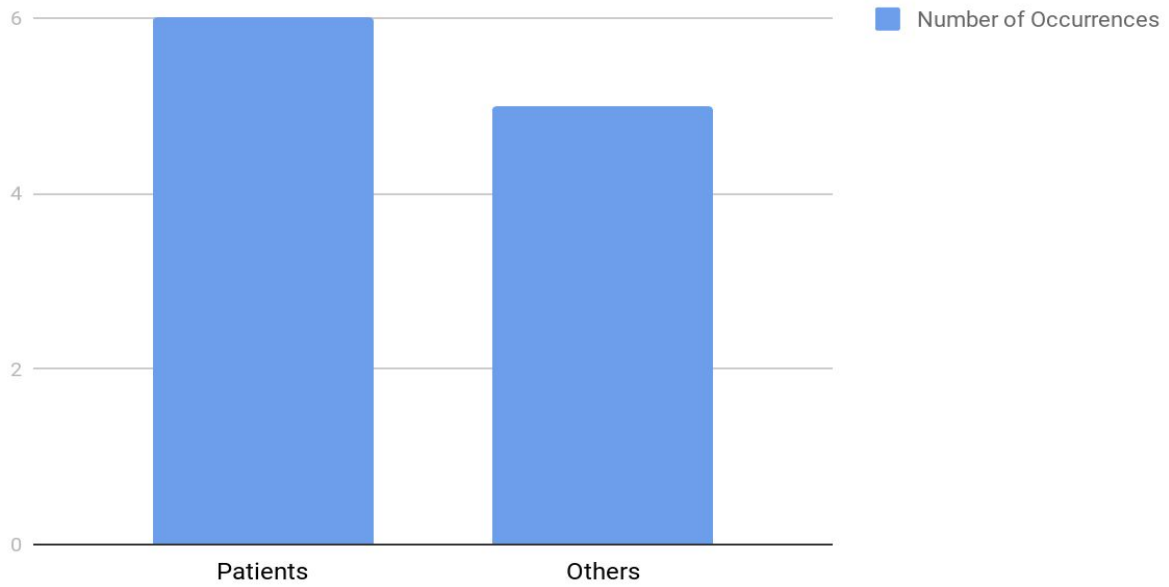


Chart 4.2 - Medical data owners as identified by patients (Simplified)

Medical Data Owners As Per Medical Professionals

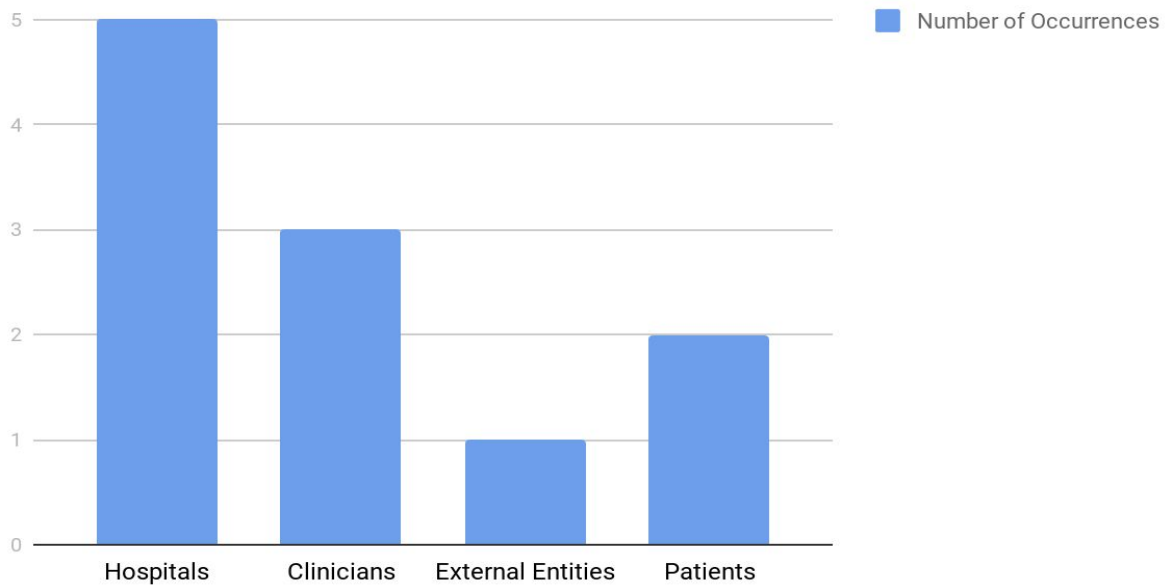


Chart 4.3 - Medical data owners as identified by medical professionals

Medical Data Owners As Per Medical Professionals (Simplified)

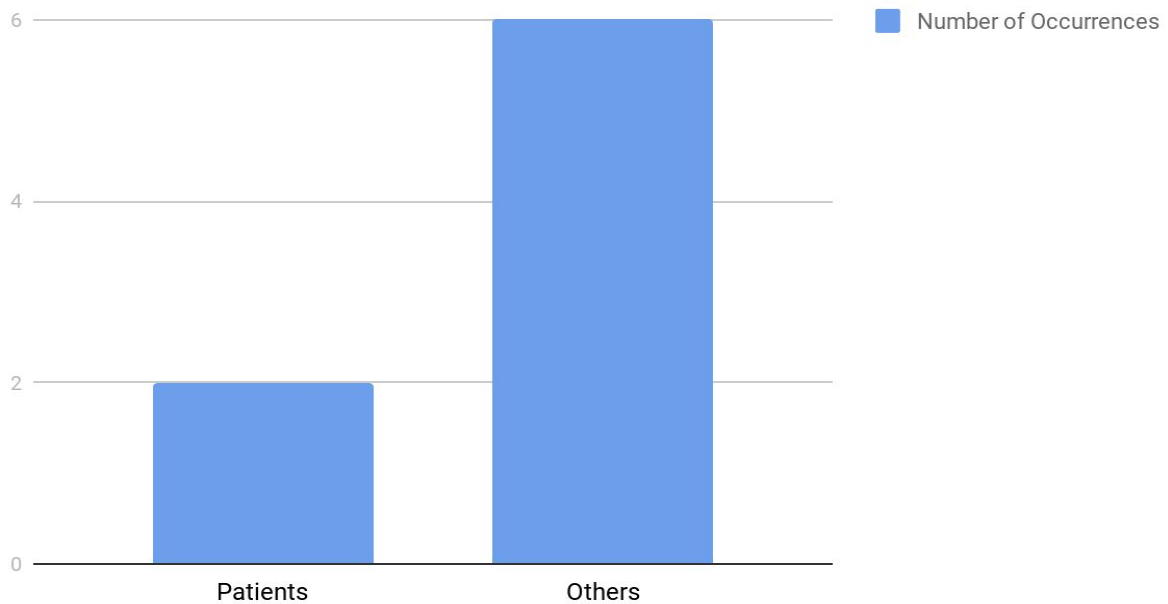


Chart 4.4 - Medical data owners as identified by medical professionals (Simplified)

4.2.2 Awareness of Medical Data Leaks

Table 4.5 lists the raw responses by each participant towards the question regarding awareness of medical data leaks. Participant group can be deduced from their code. Column deduction classifies these responses and Rationale lists reason for this classification

Code	Awareness of Medical Data Leaks	Deduction	Rationale
P-A	<i>That apply to me no, in general no, there must have been some</i>	No	
P-B	<i>Fitbit leaked whole lot of data recently</i>	Yes	
P-C	<i>I am not aware but it wouldn't surprise me if that happens</i>	No	
P-D	<i>I am not</i>	No	

P-E	<i>Yes, I am. Some records have been lost, breach in encrypted computers</i>	Yes	
P-F	<i>Not medical one, never heard of medical data leaks but have about credit cards etc.</i>	No	
P-G	<i>I am not</i>	No	
P-H	<i>Oh yeah definitely all the time, hospital systems being hacked all the time</i>	Yes	
P-I	<i>No</i>	No	
P-J	<i>No, not specifically. It's kind of back of my mind so this stuff must be happening</i>	No	It seems like the interview and previous questions caused the further response. So no is chosen as the answer
MP-A	<i>If your record is on a piece of paper it can fall anywhere. (Talks about paper based workflows)</i>	No	Participant is not aware of large scale leaks, they are referring to issues that are caused by paper based workflows
MP-B	<i>No</i>	No	
MP-C	<i>I hope no, it's a very serious issue. They have very secure computer systems It happens because of human factors</i>	No	Participant doesn't seem to be aware of any large data leaks or breaches and consider this of an internal issue
MP-D	<i>No, not data. Stories does get leaked to the press that have general interest to the public</i>	No	
MP-E	<i>No</i>	No	
MP-F	<i>Yeah, on a bigger scale there had been this NHS incident. Anecdotally you hear about this on day to day basis</i>	Yes	

Table 4.5 - Responses about awareness of medical data leaks

Chart 4.5 and 4.6 below plots the data from Table 4.5. Chart 4.5 plots number of Yes or No answers regarding knowledge of medical data leaks for both patients and medical professionals. Chart 4.6 plots these responses for all participants

Awareness of Medical Data Leaks

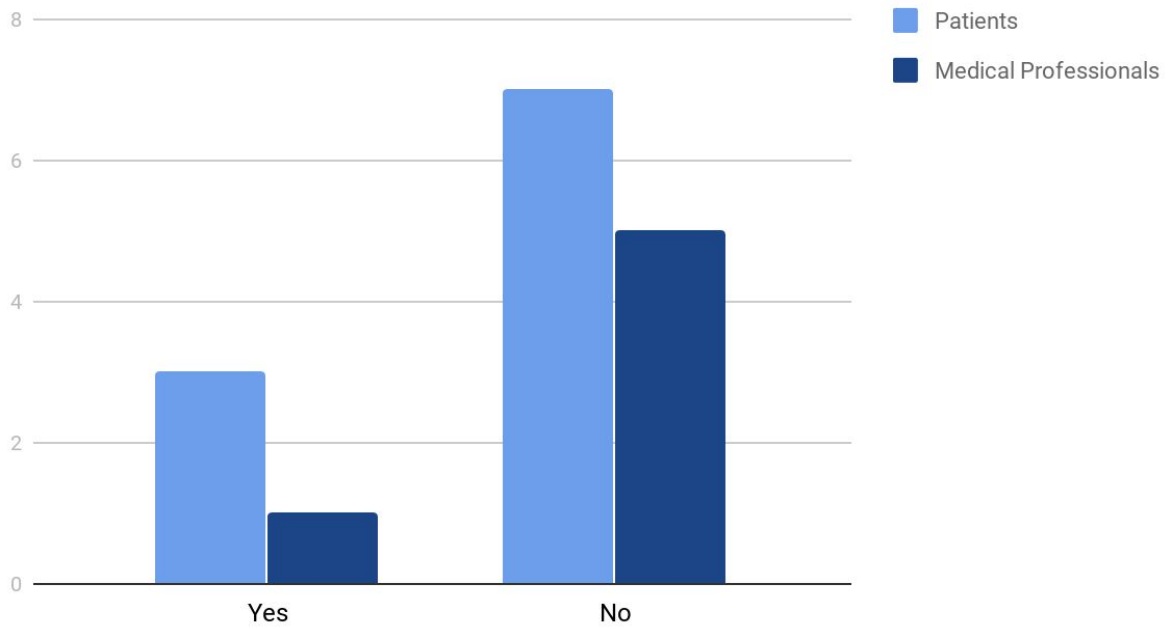


Chart 4.5 - Awareness of medical data leaks by Patients and Medical Professionals

Awareness of Medical Data Leaks (Combined)

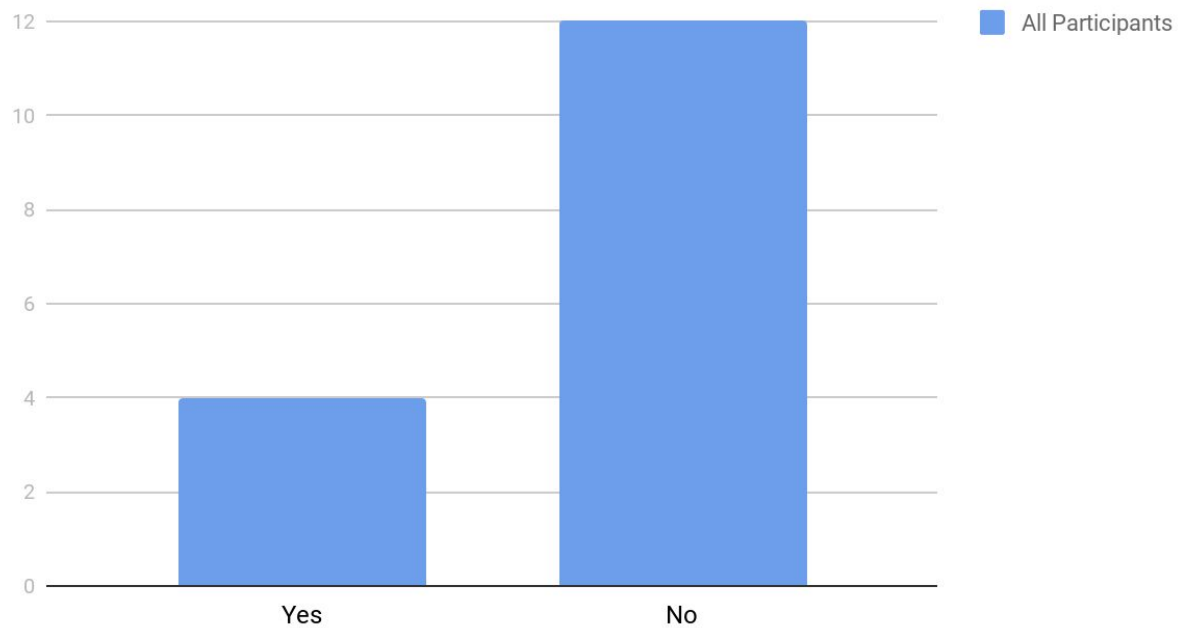


Chart 4.6 - Awareness of medical data leaks by all participants

4.2.3 Awareness of Data Privacy Laws

Table 4.6 lists the raw responses by each participant towards the question regarding awareness of data privacy laws before GDPR. Participant group can be deduced from their code. Column deduction classifies these responses and Rationale lists reason for this classification

Code	Awareness of Data Privacy Laws Before GDPR	Deduction	Rationale
P-A	<i>Yes, there's a national law CNIL, dates back to the 80s. If data is electronic it falls under CNIL</i>	Yes	
P-B	<i>Some top level idea like a glimpse</i>	No	
P-C	<i>I was aware of regulations that companies have to follow</i>	No	Participant understands data sharing guidelines in a

	<i>when handling data</i>		corporate context but not national laws
P-D	<i>None before GDPR</i>	No	
P-E	<i>Yes, Data Protection Act</i>	Yes	
P-F	<i>Yes, about HIPAA on papers for signing away rights for medical records. But I don't know the details of the law</i>	No	Participant have seen HIPAA for paperwork but they are not aware of it
P-G	<i>Not really, no</i>	No	
P-H	<i>There were some but they weren't as strict as GDPR</i>	No	
P-I	<i>Hippocratic Oath</i>	No	
P-J	<i>Not any specific laws. There's Right to be Forgotten</i>	No	
MP-A	<i>Yes, DPA</i>	Yes	
MP-B	<i>No, none before GDPR</i>	No	
MP-C	<i>Is HIPAA data privacy? We do once a year training about this</i>	Yes	Participant understands data privacy law strongly
MP-D	<i>I learn about the protocols to use in my work. Information doesn't leave the hospitals</i>	No	Participant is aware of data protocol guidelines as given by the hospital. But not about national laws
MP-E	<i>No, we are not taught these</i>	No	
MP-F	<i>On local level potential data breaches that can happen at work</i>	No	Participant is aware of policies but not a national law regarding data privacy

Table 4.6 - Responses about awareness of data privacy laws

Chart 4.7 and 4.8 below plots the data from Table 4.6. Chart 4.7 plots number of Yes or No answers regarding knowledge of data privacy laws for both patients and medical professionals. Chart 4.8 plots these responses for all participants

Awareness of Data Privacy Laws

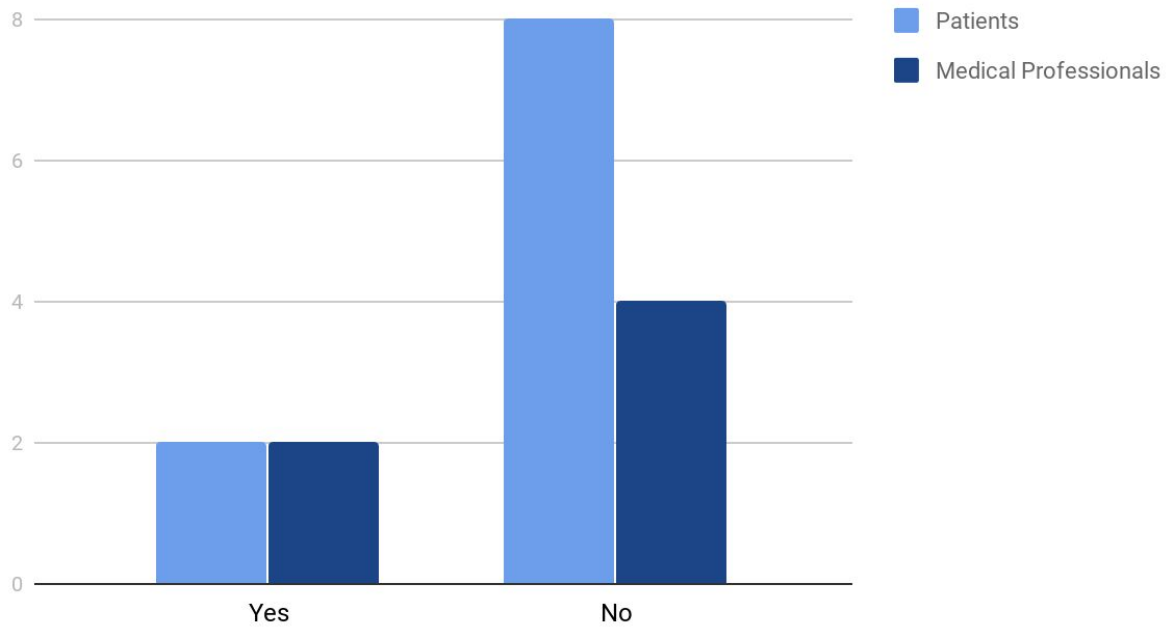


Chart 4.7 - Awareness of data privacy laws by Patients and Medical Professionals

Awareness of Data Privacy Laws (Combined)

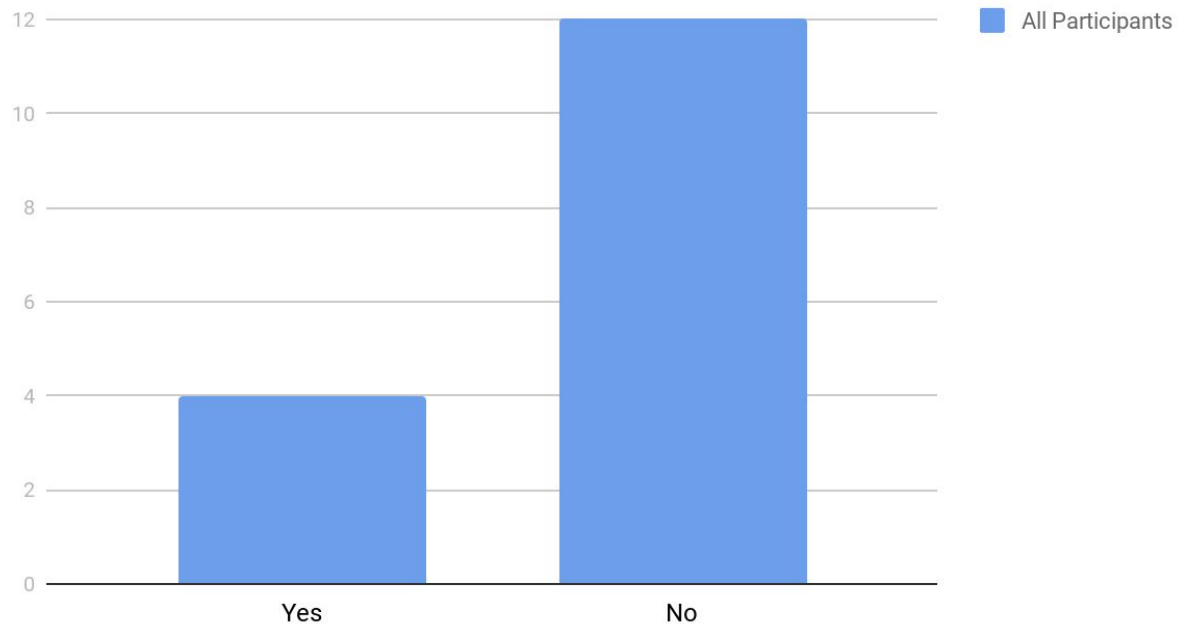


Chart 4.8 - Awareness of data privacy laws by all participants

4.2.4 Conclusion

This section intent to understand the overlap or disconnect between common questions listed in Table 3.3. Following conclusions can be drawn based on available responses

1. Patients largely identifies themselves as owners, some also considers hospitals and clinicians as **shared owners**
2. Medical Professionals do not consider patients as data owners as strongly
3. There's a common lack of awareness regarding medical data leaks
4. There's a common lack of awareness regarding data privacy laws

Qualitative nature of this study and small sample size should be taken into account. Table 4.4, 4.5 and 4.6 lists raw responses from each participant, together with their participant code that can be mapped to Table 4.1

4.3 Individual Highlights

“Fundamentally, it should be me who owns my medical data but in practice you giveaway your data and whoever has access owns the data” - Study Participant, Data Science Researcher

This section lists raw participant responses under various categories. It explores primary themes like meaning of medical data ownership, solutions as suggested by participants, concerns regarding secondary sharing and data leaks etc.

All quotes in this section are from the study participants. They are attributed and quoted using their profession, country, seniority or other background instead of participant code to give a wider context and also to aid in anonymization of responses.

4.3.1 Meaning of Medical Data Ownership

Section 2.2.3 - Data Ownership Definitions tries to find lawful definition of data ownership during literature review. There's no broadly accepted definition. The question, *what is the meaning of data ownership according to you?* was posed during the interview to some participants. This section highlights some of the responses

A participant who has worked in healthcare but identifies in the patient group has following definition

“For me owning it means, I get part of the commercial value and results of research value. Any commercial use, I approve it. Owning it also means that I consent explicitly. Going to a doctor, I am giving my data for medical purposes only”

Another participant from Ireland has following definition for the same question

“Some of my records as in what happened to me, what's wrong with me, my address and some details are owned by others”

A participant from United States has following to say

“Physical ownership, I don't pay for storage in the cloud, I don't pay for the processing of paperwork. But in terms of appropriation of its use that would be myself”

While another participant with background in insurance industry has following to say

“It’s more of that who has the actual data. I may have a copy of it. But they own what they have written down or recorded”

A student participant has the following definition

“It’s the right to use and reuse the data and archive it. But it’s a legal gray area. I am not sure if others are technically allowed to use my data for population studies”

4.3.2 Benefits and Challenges of Medical Data Ownership by Patients

Following question was asked to patient participants:

If you were to have complete ownership of your medical data in terms of

- a. Authorizing and limiting access*
- b. Being able to revoke access*
- c. Knowing the time of data usage and modifications*

What advantages and disadvantages would you perceive for you as a patient?

A similar question was asked to medical professionals

Do you have any concerns regarding patients having control over their medical data?

Both of these questions answers the research question regarding challenges of medical data ownership. This section lists corresponding responses

A participant from Ireland with years of experience in medical industry highlighted following concern

“You have to make a system with patients as data owner and be very careful how much patient is in control of the data. There need to be a happy medium. Patients may think certain information is not important but it might be. Something like being HIV Positive could be very relevant in an emergency situation”

A social entrepreneur from Ireland mentioned

“Advantages would be that employment discrimination could be avoided. It would enable me to not be treated without any bias. Disadvantages could be some people may withdraw from shared studies. But that comes back to society being more equal. If people feel safe, they will not mind sharing”

While another patient participant said

“I would like every (medical) group I work with (for medical reasons) have the same data. Revoking access, I do not care. I would prefer a more open system where I can authorize access to all (medical) data without the ability to share a part of the medical data. This may reduce possible errors”

A participant with background in research highlighted lists of concerns and challenges

“Main advantage is to know what’s going on with it. If there’s a discrimination than you are the one to blame as you must have disclosed it. You will have to understand the costs of storing and you lose features. Cloud companies can provide better reliability in that regards. You may be losing value in terms of being able to combine data and incurring costs in this regard (storage, retrieval etc)”

A participant who has recently visited a medical facility highlighted

“Advantage would be everything is in one place. No file will be missed. Same thing with appointments. They quite regularly loses files. There would be another advantage of changing location. Disadvantage would be in context of shared care. There may be concerns with sharing data from one expert to another. They might miss some important link because you decided not to disclose it”

Another participant who have worked with NHS mentioned

“Disadvantage is that it would be a hassle to manage. Advantage would be that increased transparency. If something is wrong it would come out easily. In some cases like in insurance, you may only want to disclose what is being asked specifically”


A student participant from Ireland mentioned

“It would be an advantage to control some data in context of sharing with future employers and insurance companies. They don’t need all the data. It would be good to see the connections of different entities with whom data getting shared and accessed”

4.3.3 Misuse of Medical Data

As noticed from responses in Section 4.2.2 number of patients and medical professionals that are aware of medical data leaks are low. This section quotes some of the participants regarding attitudes and concerns regarding misuse of medical data.

A former medical practitioner had following to say



"I have no idea why the medical data is more valuable than credit card data. What can they do with it? Direct danger to the person is not as big as people make it out in the media."

A participant early in their career mentioned

"I don't know why someone would want this (medical data) apart from drug companies trying to leverage on it"

Another participant who have good knowledge of data privacy laws said

"I worry about discrimination at work, access to social service. This is my main worry"

A participant from United States had following to say

"It can be misused. My first thought is about employment. Other is about insurance. It coming from bias that health insurance companies naturally decline people because of risk"

An NGO worker mentioned following concerns

"Potential insurance companies. If they get access to data they are not entitled to, it can affect my insurance claims. Someone can use some of the records for potential ID hacking"

A respondent from Ireland said the following

"Part of medical data is also held by Department of Social Protection for medical cards, rationale for why and when you are sick and accessible by some employers as well depending on context. This can be used for blackmail and there are huge amount of different ways it can be used against you"

A participant working on a senior position with a large multinational mentioned

"In general the moment someone else owns it, it can be misused. There could be bias from employers. I do not care as much about someone on the street knowing about it. I am open. But there are discrimination concerns"

A participant early in their career had following to say

"It won't affect me in this country but I think it may affect me if I was in a minority group"

4.3.4 Concerns and Attitudes Regarding Secondary Usage

Literature review and studies have highlighted concerns regarding secondary data usage with assumed consent and sharing for commercial means where original intention was personal medical care. This section highlights quotes from participants regarding secondary usage of medical data

A medical professional from Ireland mentioned

“Information should be used in the context of what patient has shared it for. If patient has come to be treated, the information should be used for treatment. If the institution wants to use that information for any kind of secondary reason then they should really get permission”

While a participant working in a multinational firm stated

“Fitbit is not a charity. Once you put a data online with a company. Full stop. They are going to monetize it. Why wouldn't they”

A more tech savvy participant shared following views regarding secondary usage

“I would prefer having control (over secondary usage) and having all (medical data) in one place integrated. Companies can buy each other and data which was not intended for some purpose or company can fall in their hand.”

When asked about monetization said

“Some hospitals does ask if you are okay to share your anonymous data for research purposes. Which I think is nice. It's about ethics and not about money. You should be able to grant explicit, time limited access”

A designer based in Ireland said the following about secondary usage

“I wouldn't mind it if I was explicitly asked. If it's for technical progress, I be inclined to share.”

And when asked about monetization said

“It's okay to share data in a charitable manner like open access, for public good”

A participant from United States mentioned

"I would like the option to revoke data access (for secondary usage). I would like to have some incentive if my data is being monetized."

A participant with background in marketing mentioned

"I would like to have control over primary and secondary usage. Any data is being used there should have transparency from A to Z. How it's being useful as outcome and where it's flowing"

Another participant with experience in working across industries internationally mentioned

"It could be hassle to approve secondary usage for every use case. I don't worry as much as I should"

And about monetization

"Monetization point is interesting. It would be good if that monetization of data can be used for social good. Often beneficiaries are stakeholders or stockholders. It doesn't mean any public good or my personal good"

A participant residing in Ireland had following to say

"I would like to have some control (over secondary usage). Opt in and out. But not as restrictive where I have to be contacted all the time. With proper explanation about the purpose"

And about monetization of data

"As long as my identity is protected, I do not care about sharing. Monetization wouldn't bother me. There's a bit of a ethical dilemma where data can be used to do harm. But I hope laws, corporate ethics will cover misuse"

4.3.5 Solutions for Medical Data Ownership by Patients

This exploratory question was asked to both medical professionals and patients group. It is part of primary research question. It was inserted to learn more about possible solutions and also to overcome any personal bias in this regards (Section 3.4). Following are raw responses from participants for *designing or implementing a solution where medical data ownership resides with patients*. Participants were told that they can go as far or as narrow and can bring or take out technical constraints

A technically inclined participant highlighted the recent attempts in area of decentralization by Tim Berners-Lee

“Silos should be split. People should be able to pick storage destination. Using OAuth etc. login grant access on demand. But this goes against the business model of big players. They will have to reinvent a bit. Check out the Tim Berners-Lee’s next project Solid. Which is targeted at breaking data silos. You can have your own private cloud or third party”

A participant who’s a designer by profession, highlighted number of broader issues with any such solution. Indeed, any such system needs to be universally accessible and usable. And that’s a considerable design constraint

“There have to be levels in any such system. You will have to think of younger and older people. What if you are not of legal age? How would they own their data? Any such system has to be designed with mindsets with cultural backgrounds taken into account. It has to have less medical words and visualizations”

A person working in an NGO has said the following. They are concerned about people not being fully informed by simple choices. They should be given visualizations behind these choices and shown the bigger picture

“System has to allow selection of data to share. It should show bigger picture in terms projecting the outcome, the perceived value in simple terms. Either numbers or visualizations. So the person can understand the value behind their actions. May be show them the building blocks especially for data sharing for research. People feel lost when they don’t have visualization behind the action. Governments have manipulated things. They have messed up before, why can’t that happen again”

A participant with the history of working with healthcare projects mentioned the following. They highlighted concerns about standardization and integration requirements for any such system.

“You have to have a standard way where data can be stored. It should be government run. It needs to be integrated with all other systems, even your phone. There’s an opportunity for a blockchain system. So everyone can draw from a system when needed and people can interact with it as needed”

A student participant highlighted that any such system shouldn’t be all at one place and patient education should be taken into account

“System can only work if it goes with the education of the users. This would be a lot about the patient education. It shouldn’t be one monolithic system. Security may suffer if it’s all in one place. It needs to have state of the art cyber protection”

A medical professional highlighted the need for security by not storing everything at one place

“Fragmentation needs to happen. If someone gets hands on a system, it should not compromise everything but may be a part of it”

4.4 Emerging Themes

Section 4.2.4 list some conclusions regarding contrasting questions (Section 4.2) (Table 3.3). Based on Section 4.3, following themes can be observed

4.4.1 Control Over Secondary Usage of Medical Data

Most participants clearly share their preference for being informed about any further medical data sharing. Although, many of them talks about greater good and ease about data sharing for research. They highlight on multiple occasions, need for entities they are sharing their data with to be explicit. If nothing else a minimum of an information form with an opt-in signature can be helpful. Some mentioned that their concern regarding secondary usage would be about identity protection. As long as that’s being met they would be fine with sharing. Option for being able to revoke access for secondary sharing was also sought by some participants.

4.4.2 Commercialization For Wider Good

Question about secondary usage was extended and asked in respect to monetization. Some participants mentioned they are aware of potential monetization of free services that are providing them some value in terms of generating reports or data storage etc. But most participants expressed intention about transparency regarding this, explicit consent and ability to revoke access later was also sought by some. Possibility of insurance premiums being lowered was also mentioned if medical data is being shared.

4.4.3 Selective Sharing of Medical Data for Insurance

Both patients and medical professional groups expressed concerns and benefits in regards to allowing patients to share medical data selectively. This naturally extend to them being owners. Number of benefits were expressed in terms of being able to avoid any potential discrimination, being in better control, better data access; losing of files by medical entities was mentioned.

Selective sharing of data with insurance companies was mentioned as a positive in multiple answers. Participants at large do not want all of their data to be shared with insurance companies but only the medical data that’s required for the purpose.



4.4.4 Ownership With Education and Responsibility Awareness

Multiple participants expressed benefits regarding owning their medical data. But concerns regarding it becoming cumbersome or added area of responsibility for them were shared. Some mentioned that it would be too much to take their permission for every usage. It may result in delay in care. Medical professionals expressed concerns regarding some data which patient may consider not to be of importance, could be important for their decisions. Concerns regarding reduced availability of medical data for research were also mentioned.

Patient education needs to be of high importance for any intervention in this direction.

4.4.5 Avoid the Monolith

When asked about implementing or designing a system with patients as medical data owners, multiple participants through varied views expressed need for systems to be modular and fragmented. From security to being able to allow better understanding in terms of building blocks and creating visualizations, this theme can be observed. This can be interpreted as a call for reducing complexity which participants already might be perceiving with existing systems.

5. Discussion

5.1 Interpretation of Results

Status quo where patients are not lawful owners of medical data is not ideal. There might be good reasons and intentions for such a setting, but this is leading to large scale system wide issues. There's a general lack of awareness on data privacy laws, abuse of data access and large scale medical data leaks. People choose medical professional for good reasons. But as learned from literature review, invisible incentives encourage them to take decisions which may not always be in best interest of patients.

Having said the above. Complete ownership where patients can omit, edit, delete the data is ideal either. When given the choice, patients do exercise omission and many of them expressed inclination to do so with non medical entities like insurance companies, during the research. During literature review it was learned that many of them exercised selective sharing with medical professionals as well.

While on one hand concerns regarding monetization and implied consent were identified both in literature review and research. The possibility of data becoming scarce for medical research was mentioned in case of ownership by patients


At the extreme both choices

1. Patients have full control and ownership
2. They have none to little control and ownership

Leads to issues. There needs to be a happy medium.

Some participants mentioned that they do not care much about their medical data. Some expressed not being adequately informed about the risks. While concerns regarding inducing fears in patients and making them paranoid about security were also shared. Some participants believe that media is overplaying the fear. But as hard statistics prove in Section 1.2, 1.3 and 2.6, if anything there's a lack of awareness. It is learned by research that both patients and medical professionals downplay these risks.

At the same time *Patrick Shanahan, Deputy Defense Secretary at Department of Defence* has made a call on (August 2018) to turn off fitness trackers and other smartphones for DoD



personnels. This is because of a leak earlier in 2018 where a fitness tracking company published maps of where users jog, bike and exercise. Many users were military personnels [117].

A situation, which clearly could have been avoided with explicit and transparent data sharing options and information. And a situation, where right to recall of previously shared data becomes important.

Secondary usage of data is a contentious issue. As noted in literature review, companies merge and buy-sell each other. An entity with whom data was shared in original spirit may not be in the position to hold that value ethically in the future. Using deanonymization techniques, this becomes an issue with possible social repercussions. Both in literature review and research interviews, participants expressed need of identity protection when sharing data. An arrangement where participants allow time based access and are made aware of their choices in detail can alleviate concerns.

As learned from literature review there are number of projects that are trying to address these issues using technological solutions. It is also learned that medical data ownership is a multifaceted problem. It is as much a legal, social and economic problem as it is technical. It is more the former than the latter. Issues surrounding corporate overreach, overprescription, data blocking, lack of portability, muddled access logs, privacy and security breaches are related to question of medical data ownership.

Any solution not only needs to empower patients, it also needs to educate them as well. It needs to take into account their background, ease of access, tech literacy and avoid the possibility of data corruption by them. At the same time there's a need of clinicians' education and awareness regarding the possible misuse of patients' data as well. Also wider societal effects of patient empowerment and education should be considered positively in light of Citizens' Jury and collaborative platforms for policy guidance.

While laws like HIPAA Omnibus Final Rule creates checks and balances in terms of highlighting patients privacy. They still does not enable and encourage a system of data portability, standardization and more choices for patients. Information blocking as an issue was raised and identified at highest levels of US administration. Something that would not have been possible with patients as owners.

5.2 Answer to the Research Question

Recalling the original research question

What are the implications, challenges and solutions for transferring medical data ownership to patients?

Implications are simply put a better, more trusted healthcare system that would not cause a sudden black swan event [117] on one fine day. It is learned that informed patients and shared decision taking leads to better health outcomes for them. Any patient or public empowerment and education can lead to possible unseen changes for the betterment of other policies as well. It can solve hosts of issues regarding privacy and security of data and address data portability and standardization issues. Lastly, it can make information blocking impossible. Allowing more choices for the patients and possibly better, proactive self management of illnesses, that can reduce pressure on healthcare systems.


There are number of **challenges** in this regard. And therefore any kind of extreme solution should be avoided. As noted, technical challenges are also economical and financial in nature. Sizable investments have been made in time and money in developing and enabling current healthcare systems. This kind of change may face opposition from multiple interests. There are number of societal issues and legal gray areas. Something as simple as patients considering themselves as owners and medical professionals do not sharing that view needs lots of work on both sides.

Solution has to come from law first. Before it can be implemented technically and concerns around patient education, selective sharing and universal design be addressed. With legal definition of patients as data owners, lots of secondary sharing abuses can be mitigated. It also sends a societal message in this regards. Abuses regarding implied consent, monetization over care can only be addressed when current medical data owners see themselves as custodians. The line about need for happy medium is worth repeating here. Solution could be something as simple as **rethinking ownership**.

To summarize, medical data ownership by patients can improve their health and health of healthcare system but any solution needs to take into account societal and legal issues. And at the same time balance the need and responsibilities of **shared data ownership** by increasing awareness on underlying issues for all involved.

5.3 Study Evaluation

Literature review highlighted concerns, challenges and benefits in greater detail and in relation to wider settings. Questions were identified based on the learnings from literature review. This helped understand the research and related questions from different angles. Many participants mentioned ideas and shared pointers and views that helped made literature review more comprehensive and subsequent interviews better. For e.g. the fact that some participants learn



about data privacy laws growing up or how they would or wouldn't be concerned about data leaks helped in identifying need to view some challenges as societal. Diversity of backgrounds in participants inspired exploration of certain themes and solutions which were not considered originally. This made the overall study incrementally better over time.

Section 6.2 lists the study limitations and section 6.4 lists opportunities for future research.

5.4 Call for Renewed Patients Rights for Medical Data

Existing laws inadequately empower medical data holders. They assume implied consent and share data further. In many cases with monetization being primary purpose. External entities mis leverage customer trust. Hosts of data leaks have been identified because of further sharing agreements.

Many of these issues can be addressed by empowering patients better, increasing tech literacy and increasing awareness of existing laws. Based on what's learned from participants and literature review, following rights for patients regarding medical data ownership should be considered

1. Right to request deletion of data in external entities
2. Right to be informed early on about potential data sharing
3. Right to invoke a prior agreement and deletion of secondary data
4. Right to proactively see audit and access logs
5. Right to share data selectively with non medical entities

6. Conclusion

This section summarizes this study and learnings. It lists study limitations, importance of this research and identifies areas for future research that could further knowledge and conversation towards medical data ownership by patients.

It finishes this study with the closing paragraph.

6.1 Summary

Research findings regarding lack of awareness concerning medical data leaks in both participant groups relates back to the original assumption that there's general lack of education on this issue. Literature review highlights that many commercial entities are more concerned about customer retention. In that respect, this outcome is understandable. There has been push for quantified self and personal data collection. Lots of investment has been made into this. As identified by both literature review and interviews that patients value their identity information highly. If the scale of medical data leaks become common knowledge, people will naturally be less inclined to collect and share data.

Similarly lack of awareness regarding data privacy laws also enables abuse of secondary usage. More informed population would demand better privacy controls. In this regard, recent GDPR ruling is a step in the right direction.

It should be highlighted once again that patients consider themselves as owners but medical professionals do not share that view. Going back to the data ownership definition in Section 2.2.3.1. This does leaves lots of discretionary power at non patient entities and as evident from various statistics shared in Section 2.6, this does causes many data handling issues.

On the other hand, speaking with various medical professionals and understanding concerns from them regarding selective sharing and possible quality issues with patient generated data, a more balanced and inclusive approach towards medical data ownership by patients should be taken. This however does not alleviate calls for selective sharing with non medical entities, being better informed about sharing agreements and to share commercialization gains from shared medical data socially.

Currently accepted definition of patients being able to access their data by being data owners needs to be expanded. Section 5.4 makes a call for certain rights in that regards and Section 5.2 answers the research question.

6.2 Study Limitations

Although patients and medical professional groups have been instrumental. At times it was felt that a connection and possibility to directly speak with some industry experts could have been beneficial. Given the time, number of participants and qualitative nature of this study some observable patterns cannot be fully concluded. It would be interesting to learn about interest in medical data ownership based on age groups, technical literacy and economic variability. Similarly a study towards attitudes in patients and medical professionals in terms of using a new system where ownership of medical data is with the patients could help elucidate on design constraints.

6.3 Importance of this Research

This research addresses the assertion that patients do not have much to gain by them being data owners. It lists hosts of issues with current data ownership regime. It highlights conclusively both through literature review and research that issues surrounding implied consent, monetization of data, lack of standards, overprescription, opposition for patients' choices and data blocking that current system is not ideal. Empowering patients in this regards and rethinking data ownership can be a good step forward to address many of these issues.

6.4 Opportunities for Future Research

Based on this research, number of areas for follow up studies in the area of medical data ownership by patients can be identified. Some of them are listed below

1. Large qualitative study with non patient entities

Medical systems are complex. They need to be legally compliant, avoid all sorts of abuse and seek to provide best care while balancing multiple motives. It would be good to do a deep interview based study with non patient entities and learn more about medical data ownership concerns and constraints

2. Design difficulties in implementing a new technical solution

How would this system function for all age groups, social and economic backgrounds, address accessibility and cultural constraints. It would be good to conduct an

experimental study with general public as medical data owners and to note their friction with medical professionals in day to day interactions

3. A quantitative study with a large sample set that can highlight patterns about questions posed regarding medical data ownership, knowledge of data leaks and data privacy laws (Table 3.3) based on variability in participants according to Country, Education Level, Professional Level as highlighted in (Table 4.1)

6.5 Final Statement

Going back to the preface, taking into account depth of literature review, concerns and statements by participants and call for a happy medium in the discussion.

The reason happy medium seems optimal is because we are used to think and accept the current way of medical data ownership. Ownership is central to the functioning of any societal or economic system. A commercially driven healthcare system where patients are not the owners of their medical data, enables possibilities of misuse and excess that are causing hosts of issues and holding back a better alternative. Solutions like Linnia and Solid are in infancy but like internet, economies of scale and vaccination; they can have far reaching possibilities. They can act as a catalyst for addressing legal, social and economical facets for full medical data ownership by patients. This may seem like a daunting task but research suggests that tipping point lies at 10% [121].

7. References

1. In J.F.K. File, Hidden Illness, Pain and Pills - NYTimes - <https://www.nytimes.com/2002/11/17/us/in-jfk-file-hidden-illness-pain-and-pills.html>
2. A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy. - KESAN, JAY P. et al
3. The Pathway to Patient Data Ownership and Better Health - Katherine A. Mikk, JD; Harry A. Sleeper; Eric J. Topol, MD
4. Ron Avignone, Ethical hacking a vital necessity to fight against healthcare ransomware, M e d . E g o n . (April 27, 2016), <http://www.medicaleconomics.com/medical-economics-blog/ethical-hacking-vital-necessity-fight-against-healthcare-ransomware>
5. Ownership of Patient's Record - Wikipedia - https://en.wikipedia.org/wiki/Medical_record#Ownership_of_patient's_record
6. Who Owns Medical Records 50 State Comparison - <http://www.healthinfolaw.org/comparative-analysis/who-owns-medical-records-50-state-comparison>
7. Summary of the HIPAA Privacy Rule - Health Information Privacy - <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>
8. Google in Health - https://www.google.com/intl/en_us/health/about/
9. Microsoft Healthvault - <https://international.healthvault.com/ie/en>
10. Apple Health - <https://www.apple.com/lae/ios/health/>
11. Legal Study on Ownership and Access to Data - EU Publications - <https://publications.europa.eu/en/publication-detail/-/publication/d0bec895-b603-11e6-9e3c-01aa75ed71a1/language-en>
12. Rights of the data subject - General Data Protection Regulation - <https://gdpr-info.eu/chapter-3/>
13. "Who Owns Health Information? - Health Information & the Law" - http://www.healthinfolaw.org/lb/download-document/6640/field_article_file
14. Patient records: The struggle for ownership - Medical Economics - <http://www.medicaleconomics.com/medical-economics/news/patient-records-struggle-ownership>
15. CMPA - Canadian Medical Protective Association - https://www.cmpa-acpm.ca/static-assets/pdf/advice-and-publications/handbooks/com_electronic_records_handbook-e.pdf

16. Who Owns the Medical Record? - CMPA -
https://www.cmpa-acpm.ca/serve/docs/ela/goodpracticesguide/pages/communication/Documentation/who_owns_the_medical_record-e.html
17. Assigning Data Ownership - Data Governance Institute -
<http://www.datagovernance.com/assigning-data-ownership/>
18. Legislation and guidance relating to medical records explained by House of Commons Library -
<http://www.nhsconfed.org/resources/2015/10/legislation-and-guidance-relating-to-medical-records-explained-by-house-of-commons-library>
19. Medical Records (Ownership and Storage) -
<https://api.parliament.uk/historic-hansard/written-answers/1976/nov/30/medical-records-ownership-and-storage>
20. Caldicott Principles - NHS - <https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx>
21. Electronic Health Record Breaches as Social Indicators - Waldemar W. Koczkodaj et al
22. Trend Micro on value and targeting of medical data -
<https://www.trendmicro.com/vinfo/ie/security/news/cyber-attacks/medical-data-in-the-crosshairs-why-is-healthcare-an-ideal-target>
23. Experian on consequences of medical data theft -
<https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf>
24. Finding a Healthier Approach to Managing Medical Data - Greengard, Samuel
25. Executable Choreographies for Medical Systems Integration and Data Leaks Prevention - Sinica Alboaie et al - IEEE
26. The Role of HIPAA Omnibus Rules in Reducing the Frequency of Medical Data Breaches: Insights From an Empirical Study - Yaraghi N et al
27. Insiders Caused Bulk of Data Breaches -
<https://www.healthcareitnews.com/news/insiders-hackers-causing-bulk-2017-healthcare-data-breaches>
28. List of Data Breaches - https://en.wikipedia.org/wiki/List_of_data_breaches
29. Healthcare Data Breach: What to Know About Them and What to Do After One - Experian -
<https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/>
30. ICO (Information Commissioner's office) data shows health sector accounts for 43 percent of all data breach incidents - <https://www.egress.com/en-US/news/ico-data-march-2017>
31. Department of Health : Investigation : WannaCry cyber attack and the NHS / UK Parliament National Audit Office

32. NHS data breach affects 150,000 patients in England - BBC - <https://www.bbc.com/news/technology-44682369>
33. Security breach fears over 26 million NHS patients - Telegraph - <https://www.telegraph.co.uk/news/2017/03/17/security-breach-fears-26-million-nhs-patient-s/>
34. Literature Review: Factors influencing health data sharing preferences of consumers: A critical review - Moon, Lisa A
35. What caused the breach? An examination of use of information technology and health data breaches - Wikina SB et al
36. Health South East RHF data breach exposed health records for half of Norway's Population - <https://securityaffairs.co/wordpress/67922/data-breach/health-south-east-rhf-databreach.html>
37. Report on Health Information Blocking - The Office of the National Coordinator for Health Information Technology (ONC) - https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf
38. Unpatients—why patients should own their medical data - Leonard J Kish & Eric J Topol
39. Sir Tim Berners-Lee speaks out on data ownership - The Guardian - <https://www.theguardian.com/technology/2014/oct/08/sir-tim-berners-lee-speaks-out-on-data-ownership>
40. Obama Administration Report Slams Digital Health Records - WSJ - <https://www.wsj.com/articles/report-slams-digital-health-records-1428638879?KEYWORDS=medical+records+Obama>
41. Health data coop - <https://www.healthbank.coop/>
42. Much Ado About Data Ownership - Barbara J. Evans - Harvard Journal of Law & Technology Volume 25, Number 1 Fall 2011
43. Patient Perspectives on Sharing Anonymized Personal Health Data Using a Digital System for Dynamic Consent and Research Feedback: A Qualitative Study - Karen Spencer, PhD et al
44. The Blockbuster Drug of the Century: An Engaged Patient - <http://healthstandards.com/blog/2012/08/28/drug-of-the-century/>
45. Health Data Exploration Project. Personal data for the public good: new opportunities to enrich understanding of individual and population health
46. Most patients are willing to share health data, engage online. EHR Intelligence - Bresnick J. - <https://ehrintelligence.com/news/most-patients-are-willing-to-share-health-data-engage-online/>

-
47. Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability - Deloitte , Directorate-General for Communications Networks, Content and Technology - EU Publications -
<https://publications.europa.eu/en/publication-detail/-/publication/08e03d91-4835-11e8-be1d-01aa75ed71a1/language-en>
 48. How engaged are consumers in their health and health care, and why does it matter - Hibbard JH et al
 49. 2011 Survey of Health Care Consumers in the United States Key Findings, Strategic Implications -
http://www.statecoverage.org/files/Deloitte_US_CHS_2011ConsumerSurveyinUS_062111.pdf
 50. Moving Beyond The Patient Data Ownership Debate -
<https://www.carecloud.com/continuum/patient-data-ownership-debate/>
 51. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules -
<https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf>
 52. A Revolution in Healthcare is Coming - The Economist -
<https://www.economist.com/leaders/2018/02/01/a-revolution-in-health-care-is-coming>
 53. How many deaths could have been avoided in the EU? - EuroStat -
<http://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20170614-1>
 54. "Depressingly frequent" preventable deaths in hospitals can be avoided with data sharing -
<https://www.healthcareit.com.au/article/depressingly-frequent-preventable-deaths-hospitals-can-be-avoided-data-sharing>
 55. Inviting Patients to Read Their Doctors' Notes: A Quasi-experimental Study and a Look Ahead - Tom Delbanco, MD et al
 56. Facebook tried to access and match medical data – report - The Register -
https://www.theregister.co.uk/2018/04/06/facebook_tried_to_slurp_medical_data/
 57. Robust De-anonymization of Large Sparse Datasets - Arvind Narayanan and Vitaly Shmatikov
 58. Structural Data De-anonymization: Quantification, Practice, and Implications - Shouling Ji et al
 59. Health Record Audit Trails: How Useful is the Metadata that is Associated with a Patient's Health Record? -
<https://www.nhdlaw.com/health-record-audit-trails-useful-metadata-associated-patients-health-record/>

-
60. The third-leading cause of death in US most doctors don't want you to know about - CNBC - <https://www.cnn.com/2018/02/22/medical-errors-third-leading-cause-of-death-in-america.html>
 61. Medical error—the third leading cause of death in the US - BMJ - <https://www.bmj.com/content/353/bmj.i2139>
 62. Letter to CDC - Re: Methodology Used to Collect National Health Statistics - <https://www.documentcloud.org/documents/2822345-Hopkins-CDC-letter.html>
 63. Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper - Charles Safran, MD, MS et al
 64. Will the IoT Bring a Patient Engagement, Interoperability Revolution? - Health Analytics - <https://healthitanalytics.com/features/will-the-iot-bring-a-patient-engagement-interoperability-revolution>
 65. GlaxoSmithKline makes \$300M investment in 23andMe, forms 50-50 R&D pact - Fierce Biotech - <https://www.fiercebiotech.com/biotech/glaxosmithkline-makes-300m-investment-23andme-forms-50-50-r-d-pact>
 66. GlaxoSmithKline (GSK) Products, Lawsuits, History and Scandals - Drug Watch - <https://www.drugwatch.com/manufacturers/glaxosmithkline/>
 67. Social Care is Inherently Unsafe - British Medical Journal - 3 June 2017 - 357:371-412 No 8108| CR ISSN 0959-8138
 68. Time to put health at the heart of policy making - British Medical Journal - 10 June 2017 - 357:413-454 No 8109|CR ISSN 0959-8138
 69. Future Earth - linking research on health and environmental sustainability - British Medical Journal - 3 June 2017 - 357:371-412 No 8108| CR ISSN 0959-8138
 70. Are citizens' juries good for our health? - 10 June 2017 - 357:413-454 No 8109|CR ISSN 0959-8138
 71. Data sharing statements for clinical trials - A requirement of the Internal Committee of Medical Journal Editors - 10 June 2017 - 357:413-454 No 8109|CR ISSN 0959-8138
 72. Who Owns the Data? Open Data for Healthcare - Patty Kostkova et al
 73. Regulator evaluation of biosimilars throughout their product lifecycle - Hye-Na Kang et al - WHO Bulletin - Hye-Na Kang et al
 74. Lessons from the field - Post-earthquake health-service support, Nepal - Sophie Goyet et al - WHO Bulletin - Volume 96, Issue 4, April 2018, 225-296
 75. Update on the Global Charter for the Public's Health - Bettina Borisch et al
 76. The diffusion of virtual communities in health care: Concepts and challenges - George Demiris
 77. e-Health Cloud: Opportunities and Challenges - AbuKhoua, Eman et al

-
78. The Standard Health Record - <https://www.standardhealthrecord.org>.
 79. What the Most Common Passwords of 2016 List Reveals [Research Study] - Keeper Security - <https://keepersecurity.com/blog/2017/01/13/most-common-passwords-of-2016-research-study/>
 80. Give GPs access to urgent CT scans - British Medical Journal - 17 June 2017 - 357:455-496 No 8110|CR ISSN 09
 81. Chinese AI Beats Doctors in Diagnosing Brain Tumors - Popular Mechanics - <https://www.popularmechanics.com/technology/robots/a22148464/chinese-ai-diagnosed-brain-tumors-more-accurately-physicians/>
 82. Solid - Social Linked Data - <https://solid.mit.edu/>
 83. Prescribing incentives feel grubby because they are - Margaret McCartney - British Medical Journal - 10 June 2017 - 357:413-454 No 8109|CR ISSN 0959-8138
 84. Building resilient health systems: a proposal for a resilience index - Margaret E Kruk et al
 85. Improving public health information for patients: shared decision making and influenza vaccination - Tudrej BV et al
 86. 23andMe Sold Access to Your DNA Library to Big Pharma, But You Can Opt Out - Motherboard - https://motherboard.vice.com/en_us/article/xwkaz3/23andme-sold-access-to-your-dna-library-to-big-pharma-but-you-can-opt-out
 87. Canada is using Ancestry DNA websites to help it deport people - VICE - https://news.vice.com/en_ca/article/wjxmy/canada-is-using-ancestry-dna-websites-to-help-it-deport-people
 88. Who Controls Your Health Data? - Doug Pollack - CSO, ID Experts - Forbes - <https://www.forbes.com/sites/ciocentral/2012/08/01/who-controls-your-health-data/#3a3aec76bb94>
 89. Who Owns Patient Data In Electronic Health Records? - Redux - Doug Pollack - CSO, ID Experts - <https://www2.idexpertscorp.com/knowledge-center/single/who-owns-patient-data-in-electronic-health-records-redux>
 90. Many Patients Would Like To Hide Some Of Their Medical Histories From Their Doctors - Fastcompany - <https://www.fastcompany.com/3042699/many-patients-would-like-to-hide-some-of-their-medical-histories-from-their-doctors>
 91. Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: results from a mixed methods study - Chrysanthi Papoutsis et al
 92. History of the World - Seven Cheap Things - Book - Raj Patel et al

-
93. Agroecological Farming - Groundswell International - <https://www.groundswellinternational.org/approach/agroecological-farming/>
 94. A migrant GP on upfront NHS charges - Roghieh Dehghan - British Medical Journal
 95. GP at Hand - NHS Doctor Appointments Online - <https://www.gpathand.nhs.uk/>
 96. GPs start legal fight over app service - British Medical Journal - 18 November 2017 - 359:253-294 No 8130 | CR ISSN 0959-8138
 97. National commitment to shared decision making - Leng G et al
 98. Has the Mental Health Act had its day? - BMJ 2017;359:j5248
 99. Blockchain distributed ledger technologies for biomedical and health care applications - Tsung-Ting Kuo et al
 100. Linnia - Self-Sovereignty Over Data - <http://linnia.com/>
 101. The ethics economy - Fjord Trends 2018 - <https://trends.fjordnet.com/the-ethics-economy/>
 102. Google tops Apple as world's most valuable brand - USA Today - <https://eu.usatoday.com/story/money/business/2018/05/29/google-tops-apple-worlds-most-valuable-brand/650548002/>
 103. Anne Wojcicki (CEO and Co-Founder, 23andMe) announcing GSK investment on Twitter - <https://twitter.com/annevoj23/status/1022126051210584064>
 104. Hacker News Discussion on 23andMe and GSK investment - <https://news.ycombinator.com/item?id=17609906>
 105. Hippocratic Oath - https://en.wikipedia.org/wiki/Hippocratic_Oath
 106. Medical tourism: An emerging global healthcare industry - Debra S. Sandberg et al
 107. Intel CEO Says Data is the New Oil - Fortune - <http://fortune.com/2018/06/07/intel-ceo-brian-krzanich-data/>
 108. Your medical record is worth more to hackers than your credit card - Reuters - <https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924>
 109. Dick Durbin asks a pointed question and we learn how much the Facebook founder cares about his own privacy - Inc - <https://www.inc.com/minda-zetlin/mark-zuckerberg-hearings-facebook-dick-durbin-privacy-concerns.html>
 110. 2017 Cost of Data Breach Study - Ponemon Institute and IBM Security - https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf
 111. Using It or Losing It? The Case for Data Scientists Inside Health Care - NEJM Catalyst - <https://catalyst.nejm.org/case-data-scientists-inside-health-care/>
 112. 5.6M Patient Records Breached in 2017, as Healthcare Struggles to Proactively Protect Health Data - Protenus -

<https://www.protenus.com/press/press-release/56m-patient-records-breached-in-2017-as-healthcare-struggles-to-proactively-protect-health-data>

113. Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data - Ponemon Institute and ID Experts -

<https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf>

114. Facebook CEO Mark Zuckerberg to Capitol Hill: 'It was my mistake, and I'm sorry.' - Washington Post -

<https://www.washingtonpost.com/news/the-switch/wp/2018/04/09/facebook-chief-executive-mark-zuckerberg-to-captiol-hill-it-was-my-mistake-and-im-sorry>

115. A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy. - KESAN, JAY P. et al

116. Turn Off Your Fitbit, Garmin, Apple Watch GPS NOW! -

<https://breakingdefense.com/2018/08/turn-off-your-fitbit-garmin-apple-watch-gps-now/>

117. Black Swan Theory - https://en.wikipedia.org/wiki/Black_swan_theory

118. Review of Data Security, Consent and Opt-Outs - National Data Guardian for Health and Care -

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF

119. Solid's Github Repository - <https://github.com/solid/solid>

120. Introducing Linnia -

<https://github.com/ConsenSys/linnia-resources/blob/master/introducing-linnia.pdf>

121. Minority rules: Scientists discover tipping point for the spread of ideas - Science Daily -

<https://www.sciencedaily.com/releases/2011/07/110725190044.htm>

Appendices

A. Abbreviations

Term	Full Form
HIPAA	Health Insurance Portability and Accountability Act
CMPA	Canadian Medical Protective Association
PHR	Personal Health Record
EHR	Electronic Health Record
SDM	Shared Decision Making
HITECH	Health Information Technology for Economic and Clinical Health
NICE	The National Institute for Health and Care Excellence
NHS	National Health Service
GDPR	General Data Protection Regulation
DPA	Data Protection Act
CNIL	Commission nationale de l'informatique et des libertés
PHD	Personal Health Data
EMR	Electronic Medical Record
CDC	Centers for Disease Control and Prevention

B. Glossary

1. **Data Ownership:** act of having legal rights and complete control over a single piece or set of data elements. It defines and provides information about the rightful owner of data assets and the acquisition, use and distribution policy implemented by the data owner.
2. **Data Access:** refers to software and activities related to storing, retrieving, or acting on data housed in a database or other repository. Data access crucially involves authorization to access different data repositories. Data access can help distinguish the abilities of administrators and users.
3. **Secondary Usage:** Secondary data refers to data that was collected by someone other than the user. Secondary usage of data is to utilize the data for another purpose by the data collector than understood or authorized by the user.
4. **De-anonymization:** is a strategy in data mining in which anonymous data is cross-referenced with other sources of data to re-identify the anonymous data source.
5. **Data Protection:** legal control over access to and use of data stored in computers.
6. **Data Anonymization:** is a type of information sanitization whose intent is privacy protection. It is the process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous.
7. **Identity Theft:** the fraudulent practice of using another person's name and personal information in order to obtain credit, loans, etc.
8. **Genomic Data:** refers to the genome and DNA data of an organism. They are used in bioinformatics for collecting, storing and processing the genomes of living things. Genomic data generally require a large amount of storage and purpose-built software to analyze

C. Figures, Tables and Charts

a. List of Figures

Reference	Description	Page Number
Figure 1.1	Cost of data leak per capita, 2017	11
Figure 1.2	Root cause of data breaches, 2017	13
Figure 1.3	Security threats that worry healthcare organizations, 2016	14
Figure 1.4	Security threats that worry business associates, 2016	15
Figure 1.5	Department accountable for data breach incident response, 2016	16
Figure 2.1	Screenshot of G-Suite for Healthcare offering by Google	25
Figure 2.2	Screenshot of Microsoft Healthvault product by Microsoft	25
Figure 2.3	Apple Health is a comprehensive health data platform by Apple	26
Figure 2.4	23andMe is a genome sequencing service with investments from Google	26
Figure 2.5	Medical data ownership laws in the United States	29
Figure 2.6	Who do patients trust?	34
Figure 2.7	Usefulness of personal health records for researchers	35
Figure 2.8	Share of avoidable deaths in light of current medical knowledge and technology	37
Figure 2.9	Core services are protection, prevention and promotion. Enabler functions are information, capacity, advocacy and governance	43
Figure 2.10	Types of privacy breach incidents and number of patients affected by them	45
Figure 2.11	Screenshot of tweet by Anne Wojcicki, CEO, 23andMe; announcing GSK investment	48
Figure 2.12	Screenshots of most popular responses to Anne Wojcicki's tweet	48-49




Figure 2.13	Screenshots of top Hacker News comments on GSK's investment in 23andMe	49
Figure 2.14	Answer to the question "can I stop taking part in 23andMe Research?" in 23andMe consent form	50
Figure 2.15	Screenshot of researcher's (a customer) query to 23andMe for explicit opt-out option	50

b. List of Tables

Reference	Description	Page Number
Table 2.1	Categories of medical data	22
Table 2.2	Relationship between medical data type, data creator, processor and consumer	23
Table 3.1	Questions for Patients and Rationale for inclusion	54-55
Table 3.2	Questions for Medical Professionals and Rationale for inclusion	55-56
Table 3.3	Common questions in both groups	56
Table 4.1	List of patient participants, their code and some background indicators	60-61
Table 4.2	List of medical professional participants, their code and some background indicators	61
Table 4.3	Details about education and professional level indicators	61-62
Table 4.4	Responses about medical data ownership	62-64
Table 4.5	Responses about awareness of medical data leaks	66-67
Table 4.6	Responses about awareness of data privacy laws	69-70

c. List of Charts

Reference	Description	Page Number
Chart 4.1	Medical data owners as identified by patients	64
Chart 4.2	Medical data owners as identified by patients (Simplified)	65
Chart 4.3	Medical data owners as identified by medical professionals	65
Chart 4.4	Medical data owners as identified by medical professionals (Simplified)	66
Chart 4.5	Awareness of medical data leaks by Patients and Medical Professionals	68
Chart 4.6	Awareness of medical data leaks by all participants	69
Chart 4.7	Awareness of data privacy laws by Patients and Medical Professionals	71
Chart 4.8	Awareness of data privacy laws by all participants	72

D. Ethics Approval Application

School of Computer Science & Statistics Research Ethics Application

Part A

Project Title: Towards Medical Data Ownership by Patients: Implications, Challenges and Solutions

Name of Lead Researcher (student in case of project work): Mohit Aggarwal

Name of Supervisor: Dr. Lucy Hederman

TCD E-mail: aggarwam@tcd.ie

Contact Tel No.: 0877656743

Course Name and Code (if applicable): MSc Health Informatics

Estimated start date of survey/research: 3 July 2018

I confirm that I will (where relevant):

- Familiarize myself with the Data Protection Act and the College Good Research Practice guidelines http://www.tcd.ie/info_compliance/dp/legislation.php;
- Tell participants that any recordings, e.g. audio/video/photographs, will not be identifiable unless prior written permission has been given. I will obtain permission for specific reuse (in papers, talks, etc.)
- Provide participants with an information sheet (or web-page for web-based experiments) that describes the main procedures (a copy of the information sheet must be included with this application)
- Obtain informed consent for participation (a copy of the informed consent form must be included with this application)
- Should the research be observational, ask participants for their consent to be observed
- Tell participants that their participation is voluntary
- Tell participants that they may withdraw at any time and for any reason without penalty
- Give participants the option of omitting questions they do not wish to answer if a questionnaire is used
- Tell participants that their data will be treated with full confidentiality and that, if published, it will not be identified as theirs
- On request, debrief participants at the end of their participation (i.e. give them a brief explanation of the study)
- Verify that participants are 18 years or older and competent to supply consent.
- If the study involves participants viewing video displays then I will verify that they understand that if they or anyone in their family has a history of epilepsy then the participant is proceeding at their own risk
- Declare any potential conflict of interest to participants.
- Inform participants that in the extremely unlikely event that illicit activity is reported to me during the study I will be obliged to report it to appropriate authorities.
- Act in accordance with the information provided (i.e. if I tell participants I will not do something, then I will not do it).

Signed:

Mohit Aggarwal

Date: 29 June, 2018

Lead Researcher/student in case of project work

Part B

<i>Please answer the following questions.</i>		<i>Yes/No</i>
Has this research application or any application of a similar nature connected to this research project been refused ethical approval by another review committee of the College (or at the institutions of any collaborators)?		No
Will your project involve photographing participants or electronic audio or video recordings?		No
Will your project deliberately involve misleading participants in any way?		No
Does this study contain commercially sensitive material?		No
Is there a risk of participants experiencing either physical or psychological distress or discomfort? If yes, give details on a separate sheet and state what you will tell them to do if they should experience any such problems (e.g. who they can contact for help).		No
Does your study involve any of the following?	Children (under 18 years of age)	No
	People with intellectual or communication difficulties	No
	Patients	Yes

**School of Computer Science and Statistics
Research Ethical Application Form**

Details of the Research Project Proposal must be submitted as a separate document to include the following information:

1. Title of project
2. Purpose of project including academic rationale
3. Brief description of methods and measurements to be used
4. Participants - recruitment methods, number, age, gender, exclusion/inclusion criteria, including statistical justification for numbers of participants
5. Debriefing arrangements
6. A clear concise statement of the ethical considerations raised by the project and how you intend to deal with them
7. Cite any relevant legislation relevant to the project with the method of compliance e.g. Data Protection Act etc.

Part C

I confirm that the materials I have submitted provided a complete and accurate account of the research I propose to conduct in this context, including my assessment of the ethical ramifications.

Signed: Mohit Aggarwal Date: 29 June, 2018
Lead Researcher/student in case of project work

There is an obligation on the lead researcher to bring to the attention of the SCSS Research Ethics Committee any issues with ethical implications not clearly covered above.

Part D

If external or other TCD Ethics Committee approval has been received, please complete below.

External/TCD ethical approval has been received and no further ethical approval is required from the School's Research Ethical Committee. I have attached a copy of the external ethical approval for the School's Research Unit.

Signed: Date:
Lead Researcher/student in case of project work

Part E

If the research is proposed by an undergraduate or postgraduate student, please have the below section completed.

I confirm, as an academic supervisor of this proposed research that the documents at hand are complete (i.e. each item on the submission checklist is accounted for) and are in a form that is suitable for review by the SCSS Research Ethics Committee

Signed: Lucy Hederman Date: 29 June, 2018
Supervisor

Completed application forms together with supporting documentation should be submitted electronically to the online ethics system - https://webhost.tchpc.tcd.ie/research_ethics/ When your application has been reviewed and approved by the Ethics committee, hardcopies with original signatures should be submitted to the School of Computer Science & Statistics, Room 104, Lloyd Building, Trinity College, Dublin 2.

CHECKLIST

Please ensure that you have submitted the following documents with your application:

1.	<ul style="list-style-type: none"> • SCSS Ethical Application Form 	Yes
2.	<ul style="list-style-type: none"> • Participant's Information Sheet must include the following: <ol style="list-style-type: none"> a) Declarations from Part A of the application form; b) Details provided to participants about how they were selected to participate; c) Declaration of all conflicts of interest. 	Yes
3.	<ul style="list-style-type: none"> • Participant's Consent Form must include the following: <ol style="list-style-type: none"> a) Declarations from Part A of the application form; b) Researchers contact details provided for counter-signature (your participant will keep one copy of the signed consent form and return a copy to you). 	Yes
4.	<ul style="list-style-type: none"> • Research Project Proposal must include the following: <ol style="list-style-type: none"> a) You must inform the Ethics Committee who your intended participants are i.e. are they your work colleagues, class mates etc. b) How will you recruit the participants i.e. how do you intend asking people to take part in your research? For example, will you stand on Pearse Street asking passers-by? c) If your participants are under the age of 18, you must seek both parental/guardian AND child consent. 	Yes
5.	<ul style="list-style-type: none"> • Intended questionnaire/survey/interview protocol/screen shots/representative materials (as appropriate) 	Yes
6.	<ul style="list-style-type: none"> • URL to intended on-line survey (as appropriate) 	NA

Notes on Conflict of Interest

1. If your intended participants are work colleagues, you must declare a potential conflict of interest: you are taking advantage of your existing relationships in order to make progress in your research. It is best to acknowledge this in your invitation to participants.
2. If your research is also intended to direct commercial or other exploitation, this must be declared. For example, *"Please be advised that this research is being conducted by an employee of the company that supplies the product or service which form an object of study within the research."*

Notes for questionnaires and interviews

1. If your questionnaire is **paper based**, you must have the following **opt-out** clause on the top of each page of the questionnaire: *"Each question is optional. Feel free to omit a response to any question; however the researcher would be grateful if all questions are responded to."*
2. If you questionnaire is **on-line**, the first page of your questionnaire must repeat the content of the information sheet. This must be followed by the consent form. If the participant does not agree to the consent, they must automatically be exited from the questionnaire.
3. Each question must be **optional**.
4. The participant must have the option to '**not submit, exit without submitting**' at the final submission point on your questionnaire.
5. If you have open-ended questions on your questionnaire you must warn the participant against naming **third parties**: *"Please do not name third parties in any open text field of the questionnaire. Any such replies will be anonymized."*
6. You must inform your participants regarding **illicit activity**: *"In the extremely unlikely event that illicit activity is reported I will be obliged to report it to appropriate authorities."*

E. Interview Protocol

a. For Patients

Research Study: Towards Medical Data Ownership by Patients: Implications, Challenges and Solutions

Interviewee Code:

Date:

Location:

Interviewer: Mohit Aggarwal

Participant Information Sheet Received and Read? Yes / No

Consent form read and signed? Yes / No

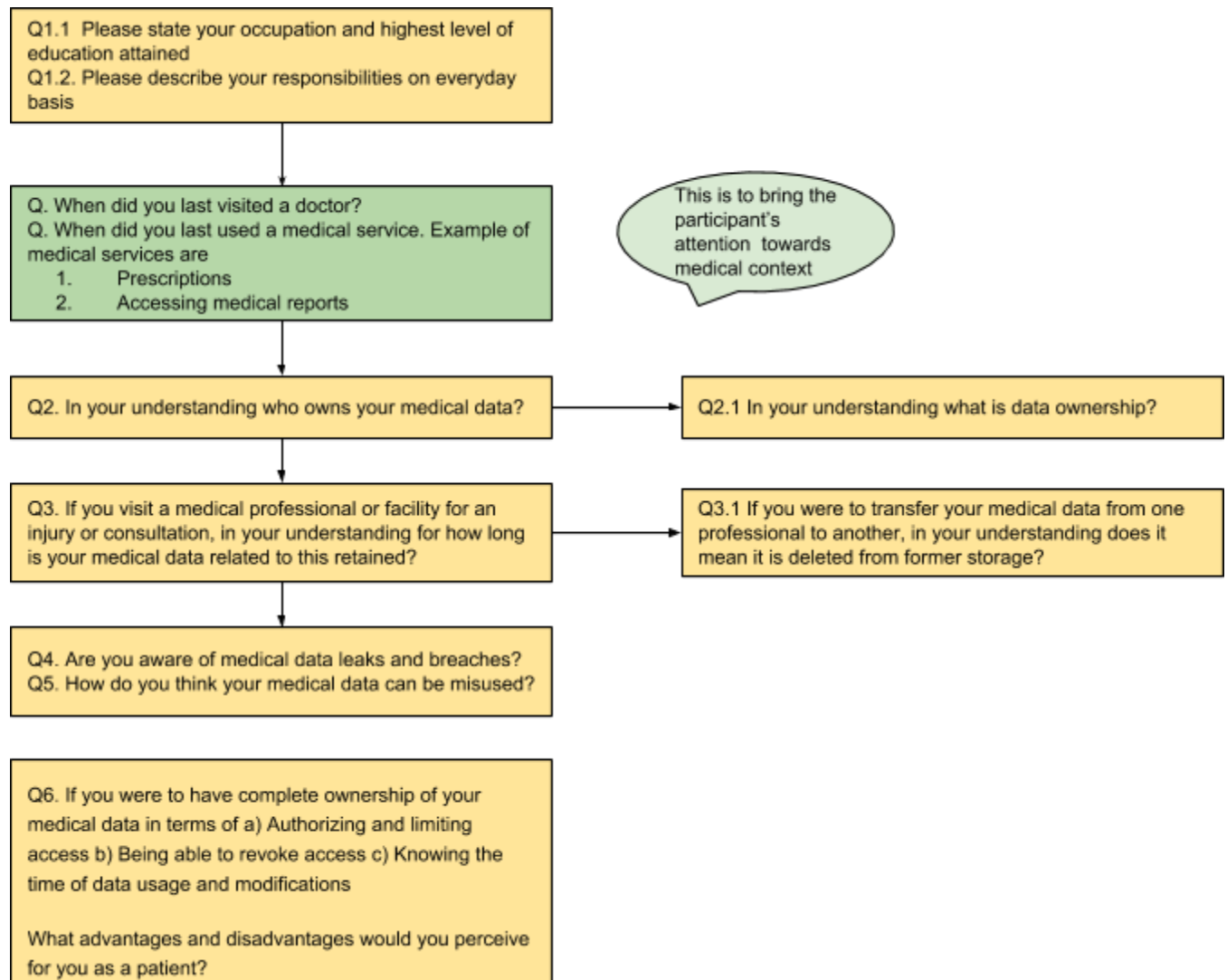
Introduction

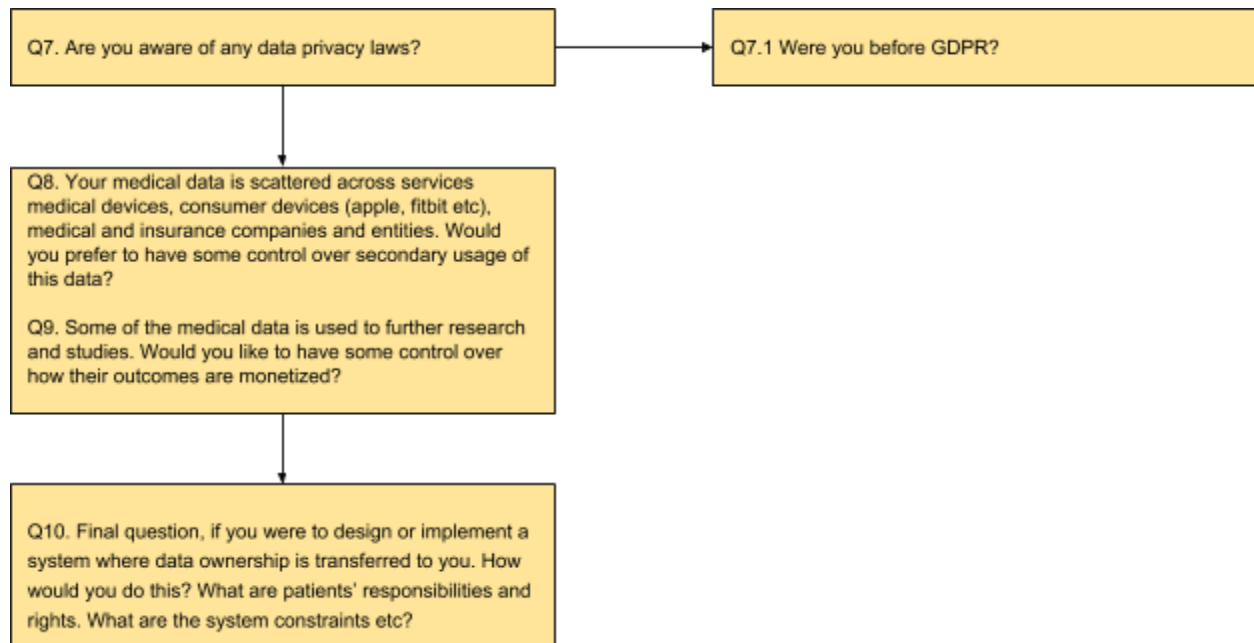
As I have explained in the information sheet, I am going to audio record our conversation today to facilitate note taking. Myself and my supervisor will be the only ones who will have access to the recording, it will be stored securely. You can request omission and deletion at anytime until the publication of the study. You can chose to not be recorded although it would be beneficial to go back to the interview at a later stage. You have been asked to sign a consent form and if you have any questions about that, I'm happy to answer them now.

Interview is expected to last around 20 minutes. I have a set of 7-10 questions. It is exploratory in nature and I may ask follow up related questions to better understand your responses and guide both of us towards the right context. Feel free to stop me at anytime or let me know if you would like not to answer a question.

We all are patients from medical services perspective. We have either used them or know someone who have. Our knowledge and understanding of the system as end users is crucial to understand the need for amendments and pain points towards medical data security. You were approached for the study as I am seeking a wide spectrum of participants with as broad a mix of demographics as possible

Interview





Debrief

If you want a copy of any of the information that I have recorded as part of this conversation or the anonymized or aggregated results, feel free to email me and I can send that to you. Also, in case you change your mind about information provided during the interview, please let me know and I will delete it. If you have any questions at a later stage please reach out to me over email, phone etc. and I will get back to you

Interview Notes

Post Interview Comments/Thoughts

b. For Medical Professionals

Research Study: Towards Medical Data Ownership by Patients: Implications, Challenges and Solutions

Interviewee Code:

Date:

Location:

Interviewer: Mohit Aggarwal

Participant Information Sheet Received and Read? Yes / No

Consent form read and signed? Yes / No

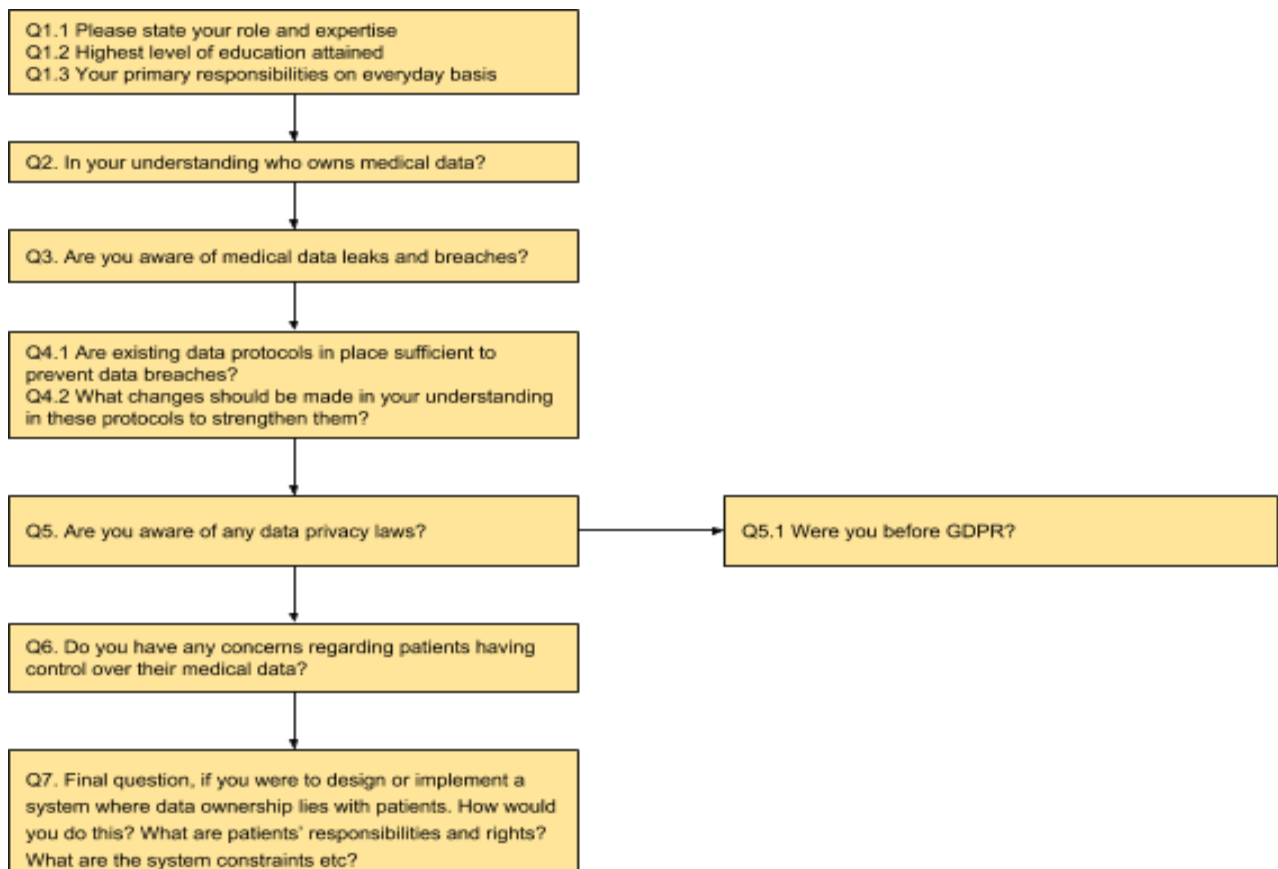
Introduction

As I have explained in the information sheet, I am going to audio record our conversation today to facilitate note taking. Myself and my supervisor will be the only ones who will have access to the recording, it will be stored securely. You can request omission and deletion at anytime until the publication of the study. You can chose to not be recorded although it would be beneficial to go back to the interview at a later stage. You have been asked to sign a consent form and if you have any questions about that, I'm happy to answer them now.

Interview is expected to last around 20 minutes. I have a set of 7-10 questions. It is exploratory in nature and I may ask follow up related questions to better understand your responses and guide both of us towards the right context. Feel free to stop me at anytime or let me know if you would like not to answer a question.

Your perspective and knowledge about medical services is crucial for this study. As primary decision taker based on available data, data creator and modifier, you can help identify accuracy of various data protocols in place. You were approached for this study as I am seeking a wide mix of professionals with different areas of responsibilities in the medical services. This would help us better understand the issues surrounding medical data security from multiple viewpoints.

Interview



Debrief

If you want a copy of any of the information that I have recorded as part of this conversation or the anonymized or aggregated results, feel free to email me and I can send that to you. Also, in case you change your mind about information provided during the interview, please let me know and I will delete it. If you have any questions at a later stage please reach out to me over email, phone etc. and I will get back to you

Interview Notes

Post Interview Comments/Thoughts

F. Information Sheet for Prospective Participants

a. For Patients

Research Study: Understanding Medical Data Ownership

Background

I would like to invite you to participate in this study, which is being undertaken as a requirement for an MSc in Health Informatics at Trinity College Dublin. Before you decide whether to take part, it is important that you know what it is about, what you will be asked to do and what the information will be used for. Please take the time to read this information leaflet and discuss it with others if needed. If you choose to participate, you will also be asked to sign a consent form. Should you decide to participate, you are free to change your mind at any point and will not need to give a reason.

What is the study about?

This study aims to understand concerns, education and frictions around medical data ownership. I am interested in conducting a semi structured, exploratory interview to note your personal views and understanding about usage, transfer and monetization of such data; that also leads to challenges around medical data security. Results of this study aims to further conversation about validity of incentives and roles around medical data ownership

Do you have to take part in the study?

Your participation is entirely voluntary.

As a end user of medical services, your perspective and concerns can be valuable to understand pain points and possible solutions as you would like it to be. Your experience and voice can be invaluable in guiding me towards further areas that should be considered for the purpose of this study

What your participation would entail?

If you are interested in participating, please let me know by contacting me at the email address or phone number that I have provided. I will contact you to arrange a time that is convenient for you to meet with me, at a location that suits you. We can also meet over Skype or conduct a phone interview if that suits better. I will record the audio of the interview, which is expected to last approximately 20 minutes. You can chose to not be recorded although it would be beneficial to

go back to the interview at a later stage. When I have completed the study, I will produce an anonymised study of findings. I will create a unique code based on your initials, profession, education etc and store the file with that name. So to be able to delete or make amendments at a later stage if you deem important. If you are interested in receiving a copy of this, I will be happy to share it with you.

Why might you want, or not want, to participate?

Our hospitals systems and services, medical and consumer devices (phones, fitbits) produce enormous amount of medical data. Understanding the constraints, advantages and disadvantages around ownership of this data is important. Your views can be highly valuable towards this cause.

If you consider this topic would not yield long term value gain for our collective understanding, you can opt out during or after the interview until the publication for any reason without penalty.

Will your responses remain confidential?

If you agree to participate in the study, your name will not be recorded or shared with third parties. Your responses will be used solely for this project and I will not have access to any other information related to your healthcare. However, in the very unlikely event that you reveal illicit activity during the interview, I will be obliged to report it to the appropriate authorities.

The interview will be recorded on a password-protected smartphone and transferred to 2FA protected Dropbox after the interview. The Dropbox shared folder is only accessible by the researcher and their supervisor. The passwords for both will only be known to the researcher and will not be shared.

The recording and responses will be solely available to the researcher and will not be played in any public forum. Your information will be anonymised and will only be identified by false names or codes. The data will be analysed by myself and the results used as part of my dissertation. I will not use any direct quotations from our conversation before first checking with you that it is ok to do so. Quotations will be cited using a reference without identifying the participant. For e.g. people from country <country name>, someone with expertise <expertise>, someone with education background <education level>. In this case, the quote would be anonymised and I would provide you with the text and context within which it will be used. If you do not want the quote to be used, or feel that the context is incorrect, then you are free to ask me to amend it or omit it entirely from the dissertation. The anonymised, aggregated results may also be used for peer reviewed journals or conference presentations. Participants will not be identifiable in any of these publications. Your information will remain strictly confidential at all times.

For the purpose of the study it would be beneficial to cite socio-economic-educational background of the participants.

None of these references will be able to identify the participant.

What should I do next?

If you are interesting in participating, please contact me to let me know. If you have any additional questions before deciding whether to participate, please feel free to contact me and I will be happy to answer them. Many thanks for reading this information sheet and for considering your participation in this study.

Why have I been asked to participate?

For the purpose of this study, it is important to speak with users of the health services. As I have clarified the usage of term patient in this regards. We all use or has used health services and systems and are aware of their workings and shortcomings. I have contacted you as you share a group with me or I have a social channel through which I can reach to you at. Your perspective and insights can be beneficial towards drawing conclusions about understanding of primary users of health services.

Conflict of Interest

Some participants are directly known and others may be known to the researcher in sense of sharing similar groups, being acquaintances etc. No participant will have direct work relationship or any shared area of influence with the researcher. Participants are sought for their expertise and diversity.

Yours sincerely,

Mohit Aggarwal

Email: [REDACTED]

Phone: [REDACTED]

b. For Medical Professionals

Research Study: Understanding Medical Data Ownership

Background

I would like to invite you to participate in this study, which is being undertaken as a requirement for an MSc in Health Informatics at Trinity College Dublin. Before you decide whether to take part, it is important that you know what it is about, what you will be asked to do and what the information will be used for. Please take the time to read this information leaflet and discuss it with others if needed. If you choose to participate, you will also be asked to sign a consent form. Should you decide to participate, you are free to change your mind at any point and will not need to give a reason.

What is the study about?

This study aims to understand concerns, education and frictions around medical data ownership. I am interested in conducting a semi structured, exploratory interview to note your personal views and understanding about usage, transfer and monetization of such data; that also leads to challenges around medical data security. Results of this study aims to further conversation about validity of incentives and roles around medical data ownership

Do you have to take part in the study?

Your participation is entirely voluntary.

As a medical professional, your understanding of medical data is comprehensive. You create, use and modify such data on everyday basis or know such protocols. It would be extremely beneficial to understand your views around medical data ownership and possible pain points as you see them.

What your participation would entail?

If you are interested in participating, please let me know by contacting me at the email address or phone number that I have provided. I will contact you to arrange a time that is convenient for you to meet with me, at a location that suits you. We can also meet over Skype or conduct a phone interview if that suits better. I will record the audio of the interview, which is expected to last approximately 20 minutes. You can chose to not be recorded although it would be beneficial to go back to the interview at a later stage. When I have completed the study, I will produce an anonymised study of findings. I will create a unique code based on your initials, profession, education etc and store the file with that name. So to be able to delete or make amendments at a

later stage if you deem important. If you are interested in receiving a copy of this, I will be happy to share it with you.

Why might you want, or not want, to participate?

Our hospitals systems and services, medical and consumer devices (phones, fitbits) produce enormous amount of medical data. Understanding the constraints, advantages and disadvantages around ownership of this data is important. Your views can be highly valuable towards this cause.

If you consider this topic would not yield long term value gain for our collective understanding, you can opt out during or after the interview until the publication for any reason without penalty

Will your responses remain confidential?

If you agree to participate in the study, your name will not be recorded or shared with third parties. Your responses will be used solely for this project and I will not have access to any other information related to your healthcare. However, in the very unlikely event that you reveal illicit activity during the interview, I will be obliged to report it to the appropriate authorities.

The interview will be recorded on a password-protected smartphone and transferred to 2FA protected Dropbox after the interview. The Dropbox shared folder is only accessible by the researcher and their supervisor. The passwords for both will only be known to the researcher and will not be shared.

The recording and responses will be solely available to the researcher and will not be played in any public forum. Your information will be anonymised and will only be identified by false names or codes. The data will be analysed by myself and the results used as part of my dissertation. I will not use any direct quotations from our conversation before first checking with you that it is ok to do so. Quotations will be cited using a reference without identifying the participant. For e.g. people from country <country name>, someone with expertise <expertise>, someone with education background <education level>. In this case, the quote would be anonymised and I would provide you with the text and context within which it will be used. If you do not want the quote to be used, or feel that the context is incorrect, then you are free to ask me to amend it or omit it entirely from the dissertation. The anonymised, aggregated results may also be used for peer reviewed journals or conference presentations. Participants will not be identifiable in any of these publications. Your information will remain strictly confidential at all times.

For the purpose of the study it would be beneficial to cite role, expertise and primary responsibilities of the participants.

None of these references will be able to identify the participant.


What should I do next?

If you are interesting in participating, please contact me to let me know. If you have any additional questions before deciding whether to participate, please feel free to contact me and I will be happy to answer them. Many thanks for reading this information sheet and for considering your participation in this study.

Why have I been asked to participate?

I have contacted you as I am aware of your professional qualifications and background. I have direct social connection with you through some electronic medium. For the purpose of this study it is important to speak with medical experts with different experience and areas of expertise. Your perspective and insights can help understand the functioning and shortcomings of health systems better.

Conflict of Interest

Some participants are directly known and others may be known to the researcher in sense of sharing similar groups, being acquaintances etc. No participant will have direct work relationship or any shared area of influence with the researcher. Participants are sought for their expertise and diversity

Yours sincerely,

Mohit Aggarwal

Email: [REDACTED]

Phone: [REDACTED]

G. Informed Consent Form

a. For Patients

Research Study: Understanding Medical Data Ownership

Lead Researcher: Mohit Aggarwal

Please read the following information about this research before you consider agreeing to the subsequent declarations or signing this consent form

Background

I would like to invite you to participate in this study, which is being undertaken as a requirement for an MSc in Health Informatics at Trinity College Dublin. Before you decide whether to take part, it is important that you know what it is about, what you will be asked to do and what the information will be used for. Please take the time to read this information leaflet and discuss it with others if needed. If you choose to participate, you will also be asked to sign a consent form. Should you decide to participate, you are free to change your mind at any point and will not need to give a reason.

What is the study about?


This study aims to understand concerns, education and frictions around medical data ownership. I am interested in conducting a semi structured, exploratory interview to note your personal views and understanding about usage, transfer and monetization of such data; that also leads to challenges around medical data security. Results of this study aims to further conversation about validity of incentives and roles around medical data ownership

Do you have to take part in the study?

Your participation is entirely voluntary.

As a end user of medical services, your perspective and concerns can be valuable to understand pain points and possible solutions as you would like it to be. Your experience and voice can be invaluable in guiding me towards further areas that should be considered for the purpose of this study

What your participation would entail?



If you are interested in participating, please let me know by contacting me at the email address or phone number that I have provided. I will contact you to arrange a time that is convenient for you to meet with me, at a location that suits you. We can also meet over Skype or conduct a phone interview if that suits better. I will record the audio of the interview, which is expected to last approximately 20 minutes. You can chose to not be recorded although it would be beneficial to go back to the interview at a later stage. When I have completed the study, I will produce an anonymised study of findings. I will create a unique code based on your initials, profession, education etc and store the file with that name. So to be able to delete or make amendments at a later stage if you deem important. If you are interested in receiving a copy of this, I will be happy to share it with you.

Why might you want, or not want, to participate?

Our hospitals systems and services, medical and consumer devices (phones, fitbits) produce enormous amount of medical data. Understanding the constraints, advantages and disadvantages around ownership of this data is important. Your views can be highly valuable towards this cause.

If you consider this topic would not yield long term value gain for our collective understanding, you can opt out during or after the interview until the publication for any reason without penalty

Will your responses remain confidential?

If you agree to participate in the study, your name will not be recorded or shared with third parties. Your responses will be used solely for this project and I will not have access to any other information related to your healthcare. However, in the very unlikely event that you reveal illicit activity during the interview, I will be obliged to report it to the appropriate authorities.

The interview will be recorded on a password-protected smartphone and transferred to 2FA protected Dropbox after the interview. The Dropbox shared folder is only accessible by the researcher and their supervisor. The passwords for both will only be known to the researcher and will not be shared.

The recording and responses will be solely available to the researcher and will not be played in any public forum. Your information will be anonymised and will only be identified by false names or codes. The data will be analysed by myself and the results used as part of my dissertation. I will not use any direct quotations from our conversation before first checking with you that it is ok to do so. Quotations will be cited using a reference without identifying the participant. For e.g. people from country <country name>, someone with expertise <expertise>, someone with education background <education level>. In this case, the quote would be anonymised and I

would provide you with the text and context within which it will be used. If you do not want the quote to be used, or feel that the context is incorrect, then you are free to ask me to amend it or omit it entirely from the dissertation. The anonymised, aggregated results may also be used for peer reviewed journals or conference presentations. Participants will not be identifiable in any of these publications. Your information will remain strictly confidential at all times.

For the purpose of the study it would be beneficial to cite socio-economic-educational background of the participants.

None of these references will be able to identify the participant.

Why have I been asked to participate?

For the purpose of this study, it is important to speak with users of the health services. As I have clarified the usage of term patient in this regards. We all use or has used health services and systems and are aware of their workings and shortcomings. I have contacted you as you share a group with me or I have a social channel through which I can reach to you at. Your perspective and insights can be beneficial towards drawing conclusions about understanding of primary users of health services.

Conflict of Interest

Some participants are directly known and others may be known to the researcher in sense of sharing similar groups, being acquaintances etc. No participant will have direct work relationship or any shared area of influence with the researcher. Participants are sought for their expertise and diversity



DECLARATION

- I am 18 years or older and am competent to provide consent.
- I have read, or had read to me, the information within this document about the research.
- I have had the opportunity to ask questions and all my questions have been answered to my satisfaction and understand the description of the research that is being provided to me.
- I agree that my data is used for scientific purposes and I have no objection that my data is published in scientific publications in a way that does not reveal my identity.
- I understand that if I make illicit activities known, these will be reported to appropriate authorities.
- I understand that I may stop electronic recordings at any time, and that I may at any time, even subsequent to my participation have such recordings destroyed (except in situations such as above).
- I understand that, subject to the constraints above, no recordings will be replayed in any public forum or made available to any audience other than the current researchers/research team.
- I freely and voluntarily agree to be part of this research study, though without prejudice to my legal and ethical rights.
- I understand that I may refuse to answer any question and that I may withdraw at any time without penalty.
- I understand that my participation is fully anonymous and that no personal details about me will be recorded.
- I have received a copy of this agreement.

Participant's Name:

Participant's Signature:

Date:

Statement of investigator's responsibility: I have explained the nature and purpose of this research study, the procedures to be undertaken and any risks that may be involved. I have offered to answer any questions and fully answered such questions. I believe that the participant understands my explanation and has freely given informed consent.

Researcher's Contact Details: Mohit Aggarwal, Email: [REDACTED]. Phone: [REDACTED]

Investigator's Signature:

Date:

b. For Medical Professionals

Research Study: Understanding Medical Data Ownership

Lead Researcher: Mohit Aggarwal

Please read the following information about this research before you consider agreeing to the subsequent declarations or signing this consent form

Background

I would like to invite you to participate in this study, which is being undertaken as a requirement for an MSc in Health Informatics at Trinity College Dublin. Before you decide whether to take part, it is important that you know what it is about, what you will be asked to do and what the information will be used for. Please take the time to read this information leaflet and discuss it with others if needed. If you choose to participate, you will also be asked to sign a consent form. Should you decide to participate, you are free to change your mind at any point and will not need to give a reason.

What is the study about?

This study aims to understand concerns, education and frictions around medical data ownership. I am interested in conducting a semi structured, exploratory interview to note your personal views and understanding about usage, transfer and monetization of such data; that also leads to challenges around medical data security. Results of this study aims to further conversation about validity of incentives and roles around medical data ownership

Do you have to take part in the study?

Your participation is entirely voluntary.

As a medical professional, your understanding of medical data is comprehensive. You create, use and modify such data on everyday basis or know such protocols. It would be extremely beneficial to understand your views around medical data ownership and possible pain points as you see them.

What your participation would entail?

If you are interested in participating, please let me know by contacting me at the email address or phone number that I have provided. I will contact you to arrange a time that is convenient for you to meet with me, at a location that suits you. We can also meet over Skype or conduct a phone interview if that suits better. I will record the audio of the interview, which is expected to last

approximately 20 minutes. You can choose to not be recorded although it would be beneficial to go back to the interview at a later stage. When I have completed the study, I will produce an anonymised study of findings. I will create a unique code based on your initials, profession, education etc and store the file with that name. So to be able to delete or make amendments at a later stage if you deem important. If you are interested in receiving a copy of this, I will be happy to share it with you.

Why might you want, or not want, to participate?

Our hospitals systems and services, medical and consumer devices (phones, fitbits) produce enormous amount of medical data. Understanding the constraints, advantages and disadvantages around ownership of this data is important. Your views can be highly valuable towards this cause.


If you consider this topic would not yield long term value gain for our collective understanding, you can opt out during or after the interview until the publication for any reason without penalty

Will your responses remain confidential?

If you agree to participate in the study, your name will not be recorded or shared with third parties. Your responses will be used solely for this project and I will not have access to any other information related to your healthcare. However, in the very unlikely event that you reveal illicit activity during the interview, I will be obliged to report it to the appropriate authorities.

The interview will be recorded on a password-protected smartphone and transferred to 2FA protected Dropbox after the interview. The Dropbox shared folder is only accessible by the researcher and their supervisor. The passwords for both will only be known to the researcher and will not be shared.

The recording and responses will be solely available to the researcher and will not be played in any public forum. Your information will be anonymised and will only be identified by false names or codes. The data will be analysed by myself and the results used as part of my dissertation. I will not use any direct quotations from our conversation before first checking with you that it is ok to do so. Quotations will be cited using a reference without identifying the participant. For e.g. people from country <country name>, someone with expertise <expertise>, someone with education background <education level>. In this case, the quote would be anonymised and I would provide you with the text and context within which it will be used. If you do not want the quote to be used, or feel that the context is incorrect, then you are free to ask me to amend it or omit it entirely from the dissertation. The anonymised, aggregated results may also be used for peer reviewed journals or conference presentations. Participants will not be identifiable in any of these publications. Your information will remain strictly confidential at all times.



For the purpose of the study it would be beneficial to cite role, expertise and primary responsibilities of the participants.

None of these references will be able to identify the participant.

Why have I been asked to participate?

I have contacted you as I am aware of your professional qualifications and background. I have direct social connection with you through some electronic medium. For the purpose of this study it is important to speak with medical experts with different experience and areas of expertise. Your perspective and insights can help understand the functioning and shortcomings of health systems better.

Conflict of Interest

Some participants are directly known and others may be known to the researcher in sense of sharing similar groups, being acquaintances etc. No participant will have direct work relationship or any shared area of influence with the researcher. Participants are sought for their expertise and diversity.



DECLARATION

- I am 18 years or older and am competent to provide consent.
- I have read, or had read to me, the information within this document about the research.
- I have had the opportunity to ask questions and all my questions have been answered to my satisfaction and understand the description of the research that is being provided to me.
- I agree that my data is used for scientific purposes and I have no objection that my data is published in scientific publications in a way that does not reveal my identity.
- I understand that if I make illicit activities known, these will be reported to appropriate authorities.
- I understand that I may stop electronic recordings at any time, and that I may at any time, even subsequent to my participation have such recordings destroyed (except in situations such as above).
- I understand that, subject to the constraints above, no recordings will be replayed in any public forum or made available to any audience other than the current researchers/research team.
- I freely and voluntarily agree to be part of this research study, though without prejudice to my legal and ethical rights.
- I understand that I may refuse to answer any question and that I may withdraw at any time without penalty.
- I understand that my participation is fully anonymous and that no personal details about me will be recorded.
- I have received a copy of this agreement.

Participant's Name:

Participant's Signature:

Date:

Statement of investigator's responsibility: I have explained the nature and purpose of this research study, the procedures to be undertaken and any risks that may be involved. I have offered to answer any questions and fully answered such questions. I believe that the participant understands my explanation and has freely given informed consent.

Researcher's Contact Details: Mohit Aggarwal, Email: [REDACTED]. Phone: [REDACTED]

Investigator's Signature:

Date:

H. Ethics Application Proposal, Revisions and Approval

Research Purpose

Aim of this study is to understand the complexities around data ownership in medical systems and services. Study aims to identify understanding of general public (patients, consumers, end users) and medical professionals around data ownership, concerns and understanding around data leaks, data privacy laws and to further identify solutions in this regard.

It is known that medical data is more valuable than financial data [4]. With changes in technology, challenges in storing, securing and transferring this data between systems in people have become complex. Over the years, there has been number of medical data breaches [5][6][7]. In 2015, 37 million people were affected in Anthem Inc. data breach. A recent 2018 study published scientific evidence that since 2008, 173M individuals have been affected in medical data breaches in USA alone [1].

In a comprehensive data privacy and consumer autonomy study [2], it is postulated that consumers are not adequately empowered. They share more data than preferable. Low level of trust in governments other data entities is noted.

Concerns around data ownership also extends to secondary usage of data. Companies collecting consumer data in silos can be acquired and merged. Given enough parameters, patient identities can be deanonymized [3]. Preliminary research suggests people's willingness to share data to further research. But they may not be fully aware of concerns this presents.

Outcome of this research should elucidate





1. Known concerns, challenges around data sharing and ownership
2. Users understanding of medical data ownership, privacy laws and misuse of such data
3. Professionals understanding of medical data ownership, transfer and access
4. Highlighting and identifying solutions and concerns in empowering users towards medical data ownership





References For Ethics Approval Application


1. <https://link.springer.com/article/10.1007/s11205-018-1837-z>
2. A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy. - KESAN, JAY P. et al
3. A methodology for the pseudonymization of medical data - Thomas Neubauer et al
4. Trend Micro on value and targeting of medical data - <https://www.trendmicro.com/vinfo/ie/security/news/cyber-attacks/medical-data-in-the-crosshairs-why-is-healthcare-an-ideal-target>
5. Experian on consequences of medical data theft - <https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf>
6. Insiders Caused Bulk of Data Breaches - <https://www.healthcareitnews.com/news/insiders-hackers-causing-bulk-2017-healthcare-data-breaches>
7. Health IT Journal - Inappropriate Access to Patient Records Spanned 14 Years - <https://www.careersinfosecurity.com/inappropriate-access-to-patient-records-spanned-14-years-a-10145>

Ethics Approval

Filename	Date Uploaded	Size
 ethics approval form combined .pdf	2018-07-02 09:57:22	707.73 KB
 Research Proposal ethics approval revision 1.pdf	2018-07-16 13:49:04	265.61 KB
 Research Proposal ethics approval revision 2.pdf	2018-07-16 18:08:20	269.76 KB
 Research Proposal ethics approval revision 3.pdf	2018-07-17 14:52:31	271 KB

Revisions History of Ethics Application

TCD REC WebApp: The status of 'Towards Medical Data Ownership by Patients: Implications, Challenges and Solutions' (497) has been updated by the Committee Inbox x  

 **rec-app-help@tchpc.tcd.ie** 25 Jul   
to me 

The status of 'Towards Medical Data Ownership by Patients: Implications, Challenges and Solutions' has been updated by the Committee.

Title: 'Towards Medical Data Ownership by Patients: Implications, Challenges and Solutions'

Applicant Name: Mohit Aggarwal

Submitted by: Mohit Aggarwal

Academic Supervisor: Lucy Hederman

Application Number: 20180701

Result of the REC Meeting: Approved

The Feedback from the Committee is as follows:

This is approved

The application can be viewed here:

https://webhost.tchpc.tcd.ie/research_ethics/?q=node/497

If amendments are required, please use the following link to edit the application and upload the changes:

https://webhost.tchpc.tcd.ie/research_ethics/?q=node/497/edit

Approval Email for Ethics Application