

Best Practices to Address Medical Identity Theft Awareness:
The Case of South African Medical Aid Members

B.L. Ah Why

2020

Best Practices to Address Medical Identity Theft Awareness: The Case of South African Medical Aid Members

by

Brandon Lawrence Ah Why

Dissertation

submitted in fulfilment of the requirements for the degree

Master of Information Technology

in the

Faculty of Engineering, the Built Environment and Technology

of

Nelson Mandela University

Supervisor: Prof. Dalenca Pottas

December 2020

DECLARATION

I, *Brandon Lawrence Ah Why*, (Student Number: 217405231), hereby declare that the dissertation for the degree Master of Information Technology is my own work and that it has not previously been submitted for assessment or completion of any postgraduate qualification to another University or for any other qualification.

SIGNATURE: *Brandon*

Brandon Lawrence Ah Why

DATE: [December 2020]

ACKNOWLEDGEMENTS

Firstly, I want to thank God for providing me with the knowledge and strength needed to persevere through my master's.

I would also like to thank the following people:

- Professor Dalenca Pottas, whose constant guidance, support, and patience throughout the completion of this research dissertation is greatly appreciated
- Nelson Mandela University for the financial assistance provided during my studies
- My language editors, Lizelle Botha and Renée van der Merwe
- My family and friends who have provided loving support and encouragement throughout the completion of this study
- The respondents in this study for the time and effort it took to share their experiences with medical identity theft

ABSTRACT

The prevalence of medical identity theft continues to increase. This is a concern for medical aid members within the South African private healthcare sector. Medical identity theft can be caused by various individuals, including internal and external role players. The deceptions involved in medical identity theft can affect medical aid members, the healthcare industry, and medical aids. Medical aid members remain unaware that they are victims of medical identity theft until they receive high medical bills or are notified by their healthcare providers. This research study focused on the lack of awareness of medical identity theft among medical aid members.

The main objective of this research study was to propose best practices that can be used to address medical aid members' awareness of medical identity theft in the South African private healthcare sector. Sub-objectives were used to achieve the main objective. The first sub-objective was to identify the parties causing and the parties affected by medical identity theft. The second sub-objective was to determine the level of medical identity theft awareness among medical aid members in the South African private healthcare sector. The third sub-objective was to identify best practices to address medical identity theft awareness. The methodology used by this exploratory research study included a convergent mixed method design, which was used to obtain quantitative and qualitative data. Data collection was completed using a literature review and a questionnaire. Data analysis and reporting made use of a qualitative content analysis, descriptive statistics, and logical argumentation.

Respondents' answers to a questionnaire about their experiences with medical identity theft provided insight into South African medical aid members' awareness of medical identity theft. The data gathered from the respondents was analysed, and themes emerged that emphasised a lack of awareness of medical identity theft among South African medical aid members. Twenty-six pre-emptive and nine retroactive best practices to address medical identity theft awareness were identified from existing literature. These best practices were cross-referenced to determine their relevance to the list of concerns about medical identity theft that emanated from the survey completed by South African medical aid members.

TABLE OF CONTENTS

Declaration	2
Acknowledgements	3
Abstract	i
Table of Contents	ii
List of Figures	vi
List of Tables	viii
List of Abbreviations and Acronyms	ix
Chapter 1 Introduction	1
1.1 Background.....	1
1.2 Problem Statement	4
1.3 Research Objectives.....	4
1.4 Research Questions	5
1.5 Research Methodology	5
1.6 Research Process.....	7
1.7 Research Methods.....	9
1.7.1 Data Collection	9
1.7.2 Data Analysis	12
1.8 Ethical Considerations	13
1.9 Conclusion	13
Chapter 2 Medical Identity Theft.....	14
2.1 Introduction	14
2.2 Private Healthcare Sector	14
2.3 Healthcare Fraud	18
2.4 Medical Identity Theft.....	20
2.5 Who Is Causing Medical Identity Theft?.....	23
2.5.1 External Fraudsters: Hackers	25
2.5.2 External Fraudsters: Perpetrators	26
2.5.3 Internal Fraudsters	27
2.5.4 Summary of the Role Players Causing Medical identity Theft	28
2.6 Consequences of Medical Identity Theft	29
2.6.1 Summary of the Consequences of Medical Identity Theft	33
2.7 Conclusion	34
Chapter 3 Level of awareness in the private healthcare sector	36
3.1 Introduction	36
3.2 Data Collection.....	36
3.2.1 Questionnaire Design	36

	3.2.2	Questionnaire Distribution	38
	3.2.3	Sampling and Respondents	38
3.3		Results Part 1 – Demographics	42
	3.3.1	Age	42
	3.3.2	Geographical province.....	43
	3.3.3	Gender	44
	3.3.4	Currently or previously a member of medical aid	44
3.4		Results Part 2 – Background	45
	3.4.1	Have you previously heard the term “medical identity theft?”	45
	3.4.2	Do you know the definition of medical identity theft?	47
	3.4.3	If ‘Yes’, how did you learn about medical identity theft?	47
	3.4.4	Actions performed if aware your medical records were lost or stolen.....	49
	3.4.5	Inaccuracies caused by medical identity theft in your medical records	51
3.5		Results Part 3 – Healthcare Provider Privacy	52
	3.5.1	Checking your medical records are accurate	52
	3.5.2	Why don’t you check?	53
	3.5.3	How do you check?	55
	3.5.4	Rate the statement of healthcare provider.....	56
	3.5.5	Importance of the following issues	57
3.6		Results Part 4 – Medical Aid Privacy	58
	3.6.1	Medical aid concern for medical identity theft.....	58
	3.6.2	If ‘No’, would you consider changing	59
	3.6.3	Do you read your Statement of Benefit (SOB)?.....	60
	3.6.4	If ‘Yes’, which one is the most important to ensure the SOB is correct?...	61
	3.6.5	Review your SOB and see a claim not recognize from your healthcare provider.....	62
	3.6.6	If ‘Yes’, to whom did you report the claim?	63
	3.6.7	Would you use a free medical identity theft monitoring service?	64
3.7		Results Part 5 – Medical Identity Theft Experience.....	65
	3.7.1	Did you allow a family member to use your personal identity?	65
	3.7.2	If ‘Yes’, why did you do this?	66
	3.7.3	If ‘Yes’, how often did you share your personal healthcare information with a family member	67
	3.7.4	Did you allow a non-family member to use your personal identity	68
	3.7.5	If ‘Yes’, why did you do this?	69
	3.7.6	If ‘Yes’, how often did you share your personal healthcare information?..	70
	3.7.7	Were you or someone a victim of medical identity theft	71
	3.7.8	If ‘Yes’, who was the identity theft victim?	72
	3.7.9	How would you describe your medical identity theft incident?	73
	3.7.10	How did you learn about medical identity theft?	75
	3.7.11	When did you learn you were a victim of medical identity theft?	76
	3.7.12	Once you became aware, did you report the incident?	77
	3.7.13	If ‘No’, why was the medical identity theft not reported?.....	78
	3.7.14	How did the medical identity theft happen	79
	3.7.15	What were the financial consequences of medical identity theft incident?	81

3.7.16	What were the medical consequences of medical identity theft incident?	83
3.7.17	What were the medical aid consequences of medical identity theft incident?	84
3.7.18	Did you or your immediate family resolve the identity theft incident?	86
3.7.19	If 'Yes', how did you resolve this medical identity theft?	87
3.7.20	If 'Yes', how long did resolving the medical identity theft take?	88
3.7.21	Cost incurred trying to resolve medical identity theft	89
3.7.22	How much time was spent trying to resolve medical identity theft incident?	90
3.7.23	Steps taken to prevent future medical identity theft incident.....	92
3.7.24	List any other issues or comments about medical identity theft.....	93
3.8	Summary	94
3.9	Conclusion	96
Chapter 4 Best Practices to Address Medical Identity Theft Awareness		97
4.1	Introduction	97
4.2	Thematic Analysis of Concerns.....	97
4.3	Approach	98
4.4	Preparation of Raw Data Files	99
4.5	Close Reading of Text	101
4.6	Creation of Categories	110
4.7	Overlapping Coding and Uncoded Text	114
4.8	Continuous Revision and Refinement of Category System	119
4.9	Best Practices for Avoidance of Medical Identity Theft	123
4.9.1	Pre-emptive measures	123
4.9.2	Retroactive measures.....	131
4.10	Relevance of the Best Practice to South African Medical Aid Members	134
4.11	Conclusion	137
Chapter 5 Conclusion		138
5.1	Introduction	138
5.2	Summary of Chapters	138
5.2.1	Chapter 1 – Introduction	138
5.2.2	Chapter 2 – Medical Identity Theft.....	138
5.2.3	Chapter 3 – Level of Awareness in the Private Healthcare Sector	138
5.2.4	Chapter 4 – Best practice to Address Medical Identity Theft Awareness	139
5.2.5	Chapter 5 Conclusion	139
5.3	Research Questions and Objectives	139
5.4	Validity	141
5.4.1	Credibility.....	142
5.4.2	Transferability.....	142
5.4.3	Dependability.....	142

5.4.4	Confirmability.....	143
5.5	Research Contribution	143
5.6	Limitations.....	144
5.7	Future Research	145
5.8	Final Word.....	146
	REFERENCE LIST	147
	APPENDIX A – Ethics Approval	162
	APPENDIX B – informed consent.....	164

LIST OF FIGURES

Figure 1.1: Research Process	8
Figure 2.1: Private Healthcare Sector Diagram	15
Figure 2.2: Role Players Causing Medical Identity Theft	23
Figure 2.3: Consequences of Medical Identity Theft.....	30
Figure 3.1: Survey Sections Parts	30
Figure 3.2: Excluded Respondents.....	40
Figure 3.3: Age.....	42
Figure 3.4: Geographical Province.....	43
Figure 3.5: Gender.....	44
Figure 3.6: Membership of Medical aid.....	44
Figure 3.7: Previous Knowledge of Medical Identity Theft?.....	46
Figure 3.8: Level of Awareness of Medical Identity Theft.....	47
Figure 3.9: Sources of Information for Medical Identity Theft.....	48
Figure 3.10: Appropriate Actions After Theft of Medical Records.....	50
Figure 3.11: Awareness of Consequences of Medical Identity Theft.....	52
Figure 3.12: Accuracy of Personal Health Information.....	53
Figure 3.13: Reasons for Not Checking Own Medical Records.....	54
Figure 3.14: How Medical Records Are Checked.....	55
Figure 3.15: Respondents' Level of Trust of Healthcare Provider Scale.....	56
Figure 3.16: Respondents' Ratings Importance Relating to Health Records Scale.....	57
Figure 3.17: Medical Aid is Concerned About Medical Identity Theft.....	58
Figure 3.18: Changing Medical Aid Membership.....	59
Figure 3.19: Level of Awareness of Content of SOB.....	60
Figure 3.20: Importance of Correct SOB Information.....	61
Figure 3.21: Reviewing Claims on SOBs.....	62
Figure 3.22: Reporting Unfamiliar Claims on SOBs.....	63
Figure 3.23: Support for Free Monitoring Service.....	64
Figure 3.24: Use of Personal Identification by Family Members.....	65
Figure 3.25: Reasons for Allowing Family Members to Use One's Personal Identity.....	66
Figure 3.26: Frequency of Sharing Personal Healthcare Information.....	68
Figure 3.27: Use of Personal Medical Identity by Non-Family Members.....	69
Figure 3.28: Reasons for Permitting Non-Family to Use Personal Identity.....	70
Figure 3.29: Frequency of Helping Non-Family Members.....	71
Figure 3.30: Do you Know Who is Victims of Medical Identity Theft.....	72
Figure 3.31: Who is Victim of Medical Identity Theft.....	73
Figure 3.32: Type of Medical Aid Theft.....	74
Figure 3.33: How Theft was Detected.....	75
Figure 3.34: Length of Time to Discover Medical Identity Theft.....	76
Figure 3.35: Report of Incidence of Medical Identity Theft.....	77
Figure 3.36: Reasons Why Medical Identity Theft Was Not Reported.....	78
Figure 3.37: Details of Occurrence of Medical Aid Theft.....	80
Figure 3.38: Financial Consequences of Medical Identity Theft.....	82
Figure 3.39: Medical Consequences of Medical Identity Theft.....	83
Figure 3.40: Medical Aid Consequences of Medical Identity Theft.....	85
Figure 3.41: Resolving the Medical Identity Theft Incident.....	86
Figure 3.42: How Medical Identity Theft Was Resolved.....	87
Figure 3.43: Length if Time to Resolve Incident.....	88
Figure 3.44: The Approximate Cost of Resolving Incidence of Medical Identity Theft.....	89
Figure 3.45: Time Spent on Resolving Issue of Medical Identity Theft.....	91

Figure 3.46: Steps to Avoid Future Medical Identity Theft.....92
Figure 4.1: Phases of Content Analysis. Adapted from (Elo & Kyngäs, 2008).....98

LIST OF TABLES

Table 2.1: Role Players Involved in Committing Medical Identity Theft	22
Table 2.2: Summary of the Role Players Causing Medical Identity Theft	28
Table 2.3: Summary of the Consequences of Medical Identity Theft.....	34
Table 3.1: List of Medical Aid Membership Counts.....	45
Table 3.2: Cost Incurred by Medical Identity Theft.....	90
Table 4.1: Themes and Concerns Pertaining to Respondents.....	91
Table 4.2: Literature Sources.....	99
Table 4.3: List of Best Practices.....	102
Table 4.4: List of Best Practices and Categories.....	110
Table 4.5: Safeguard Healthcare Documents.....	115
Table 4.6: Protect Medical Information.....	116
Table 4.7: Electronic Check.....	117
Table 4.8: Financial Check.....	118
Table 4.9: Notify Officials.....	118
Table 4.10: Awareness.....	119
Table 4.11: Pre-Emptive Best Practices.....	120
Table 4.12: Retroactive Best Practices.....	122
Table 4.13: Pre-Emptive Safeguard and Review Healthcare Documents Description and Summary.....	123
Table 4.14: Pre-Emptive Protect Medical Information Description and Summary.....	125
Table 4.15: Pre-Emptive Electronic Check Description and Summary.....	127
Table 4.16: Pre-Emptive Financial Check Description and Summary.....	129
Table 4.17: Pre-Emptive Awareness Description and Summary.....	130
Table 4.18: Retroactive Safeguard and Review Healthcare Documents Description and Summary.....	131
Table 4.19: Retroactive Financial Check Description and Summary.....	131
Table 4.20: Retroactive Notify Officials Description and Summary.....	131
Table 4.21: Relevance of Best Practices to South African Medical Aid Members.....	134
Table 5.1: Problem Statement.....	139
Table 5.2: Research Question 1 and Research Objective 1.....	139
Table 5.3: Research Question 2 and Research Objective 2.....	140
Table 5.4: Research Question 3 and Research Objective 3.....	140

LIST OF ABBREVIATIONS AND ACRONYMS

EHRs	Electronic health records
EMRs	Electronic medical records
HTTP	Hypertext Transfer Protocol Secure
ID	Identity
IT	Information Technology
MIFA	Medical Identity Fraud Alliance
NHCAA	National Health Care Anti-Fraud Association
PBHRs	Payer-based health records
PHI	Protected Health Information
PHRs	Personal health records
PR	Protected Registration
QCA	Qualitative Content Analysis
SAFPS	South African Fraud Prevention Service
SAPS	South African Police Service
SMS	Short Message Service
SOB	Statement of Benefit
URL	Uniform Resource Locator

Chapter 1 INTRODUCTION

1.1 Background

The healthcare sector consists of two subsectors, namely the public healthcare sector and the private healthcare sector (Basu, Andrews, Kishore, Panjabi, & Stuckler, 2012):

- In the public healthcare sector, public healthcare services are provided to patients by the national government.
- In the private healthcare sector, private healthcare services are provided to medical aid members by non-government service providers in the healthcare industry.

Throughout this dissertation, focus will be placed on the private healthcare sector and the involvement of medical aid members therein. Erasmus (2016) explains that “[a] medical scheme helps you to pay for your healthcare needs, such as nursing, surgery, dental work, medicine and hospital accommodation... [and] [y]ou pay monthly contributions in order to have medical cover” (p. 1).

Interchangeable terms such as health insurance, healthcare insurer, medical aid insurance, and medical aid all refer to the same concept. The term medical aid will be used throughout this dissertation.

Healthcare fraud in hospitals usually occurs when acts of deception are committed by employees in the healthcare industry, leading to medical identity theft (Amigorena, 2014; Luizzo & Scaglione, 2014; Wang, Gupta, & Rao, 2015). The occurrence of healthcare fraud is gradually increasing and affects millions of people worldwide (US Ponemon Institute, 2013).

Identity theft, also known as identity fraud, is a worldwide problem. White and Fisher (2008) define identify theft as “*the unlawful use of another’s identifying information for gain*” (p. 1). Medical identity theft is a subtype of identity theft whose prevalence is continuously growing (Mancini, 2014).

Mancini (2014) defines medical identity theft as “*a practice in which someone uses another individual’s identifying information, such as health insurance or social security number, without the individual’s knowledge or permission*” (p. 1). Medical identity theft is on the leading edge of the ever-evolving crime of identity theft, and many healthcare providers are not conscious of it (Mancini, 2014).

Chapter 1: Introduction

Hedayati (2012) notes that despite the Federal Trade Commission's "*attempts to enforce the law, the number of new identity (ID) theft victims is increasing every day across the globe*" (p. 1). As the occurrence of medical identity theft progressively increases, it has a major impact on its victims. Medical identity thieves use victims' personal healthcare information, including their medical data and prescription histories, for personal gain. This can cause substantial losses for the victims through erroneous bills and discrepancies in their medical records. As such, medical aid members are losing trust and confidence in their healthcare providers (US Ponemon Institute, 2013). Medical identity theft results in victims feeling as though their information is inadequately secured and protected.

In 2013, the US Ponemon Institute and the Medical Identity Fraud Alliance (MIFA) conducted a survey in the United States with the support of ID Experts, wherein they studied 788 adult respondents (aged 18 or over). The survey reported an increase of 19% in the prevalence of medical identity theft from 2012 to 2013. The survey further reported that 21% of the respondents had been or had a close relative who had been a victim of identity theft (US Ponemon Institute, 2013). The survey further revealed that consumers were at high risk of becoming victims of medical identity theft, which could result in financial losses or complications with their medical records (US Ponemon Institute, 2013). Furthermore, the study reported that the base rate of 19% of identity theft victims increased within one year (US Ponemon Institute, 2013). As the occurrence of medical identity theft increases, it causes various issues, such as the exposure of credit card information, social security information, and billing information as well as fraudsters claiming for medical services using victims' identities (US Ponemon Institute, 2013; US Ponemon Institute, 2015; Legotlo, Hons, Mutezo, & Hons, 2018).

When a person's information is hijacked, it can be used to commit various fraudulent acts. It can be sold on the black market and can be used to generate entirely new medical identities for potential buyers (Bodhani, 2013; Dockterman, 2013; Ogunbanjo & Makgatho, 2016). Typically, a victim's identity is sold on the black market to make a small profit, and then other criminals use this new identity for their own personal gain.

Victims of medical identity theft are faced with the daunting process of reclaiming their identities and proving to their medical aid that they were not aware that fraudulent claims were being made using their names. Rectifying issues caused by medical

Chapter 1: Introduction

identity theft can take months or years. According to the US Ponemon Institute (US Ponemon Institute, 2015), resolving these issues may require over 200 hours of work with the victim's medical aid insurance and healthcare provider. Consequently, some people manage to rectify the issues, while others choose to pay exorbitant prices to restore their identities due to time constraints.

A thorny issue arises when a perpetrator's medical history and treatment records mix with a victim's records, as this causes discrepancies in the medical health records system. This leaves the patient vulnerable and unable to receive quality medical care for as long as the issue remains unresolved. About 20% of the 807 individuals who participated in a study conducted by the US Ponemon Institute in 2012 (titled "Third Annual Survey on Medical Identity Theft") reported that their records had been accessed and modified. In a worst-case scenario, altered medical records could result in the administration of the wrong type of treatment to a legitimate patient (2012).

As previously stated, victims of medical identity theft can suffer great financial losses. Criminals often use stolen identities to buy drugs or goods or to obtain treatments, thereby ruining the victims' credit records. Moreover, victims may lose their health coverage due to discrepancies in their medical records and may have to cover legal costs if a legal dispute arises (2015). The aforementioned complications may have an adverse effect on the victims' financial statuses.

According to the South African Fraud Prevention Association, the prevalence of identity theft increased by 200% from 2009 to 2015 (Loxton, 2017). As the prevalence of medical identity theft continues to grow, the public should be made aware of the issues associated with it. The exposure of patients' private health information could place individuals in a vulnerable position and have severe financial consequences caused by inaccuracies in credit reports, fraudulent bills, and incurred legal fees. Patients whose personal information is leaked could also experience public embarrassment should their medical history contain diagnoses associated with negative stereotypes or stigmas. Additionally, Hedayati (2012) states that "*the emerging new technology and the lack of enough people's knowledge about how to protect their personal information motivates fraudsters*" (p. 10). Raising awareness about medical identity theft will enable potential victims to take the appropriate actions and put precautionary measures in place. Eva Velasquez, president and CEO of the Identity Theft Resource Center, a non-profit organization that provides education and

assistance to victims of identity theft, said the following about medical identity theft: “*I believe it is vastly under-reported and misunderstood even by victims experiencing it*” (Grant & Young, 2016). Most people are vulnerable to medical identity theft due to a lack of awareness thereof.

1.2 Problem Statement

Medical identity theft is a white-collar crime aimed at defrauding patients or insurers by tampering with records to make a profit or to receive medical services (Mancini, 2014). The estimated cost of South African medical aid fraud ranges from R3 billion to R15 billion each year (“Fraud in SA healthcare system”, 2013). Although the prevalence of healthcare fraud in South Africa is growing, medical aid members are not fully aware of this growth and its consequences (Ga, Sa, & Med, 2014). As previously indicated, the prevalence of identity theft in South Africa increased by 200% from 2009 to 2015 (Loxton, 2017). However, most medical aid members learn about identity theft only once they fall victim to it. As they are uninformed about or unaware of medical identity theft, medical aid members often fail to take precautionary measures against it. Furthermore, they are not cognisant of the appropriate steps to take should they fall victim to it. This lack of awareness among medical aid members leads to a gradual increase in instances of medical identity theft.

Thus, the problem addressed by this research is the lack of awareness of medical identity theft among medical aid members.

1.3 Research Objectives

- **Main Research Objective**

This study’s main research objective is to propose best practices that can be used to address medical aid members’ awareness of medical identity theft in the South African private healthcare sector.

- **Sub-Objectives**

To achieve the main research objective, the following secondary objectives are addressed:

1. Identify the parties causing and the parties affected by medical identity theft in the South African private healthcare sector.

2. Determine the level of medical identity theft awareness among medical aid members in the South African private healthcare sector.
3. Identify best practices to address medical identity theft awareness.

1.4 Research Questions

- **Main Research Question**

The main research question addressed by this study is:

Which best practices can be used to address medical aid members' awareness of medical identity theft in the South African private healthcare sector?

- **Sub-Questions**

To answer the main research questions, the following secondary questions are addressed:

1. Who are the parties causing and the parties affected by medical identity theft in the South African private healthcare sector?
2. What is the level of medical identity theft awareness among medical aid members in the South African private healthcare sector?
3. Which existing best practices can be used to address medical identity theft awareness?

1.5 Research Methodology

Kothari (2004) defines research methodology as “*a scientific and systematic search for pertinent information on a specific topic*” (p. 1). This entails the collection of data through surveys, interviews, reading research publications, and various other methods.

Within this study, three types of research are identified, namely exploratory, descriptive, and explanatory research. These will now be explained in more detail.

Manerikar (2014) defines exploratory research as taking place “*when a researcher has a limited amount of experience with or knowledge about a research issue*” (p. 95). An advantage of exploratory research is that it provides new insights into the research topic.

Chapter 1: Introduction

Given (2011) defines descriptive research as “*a detailed account of a social setting, a group of people, a community, a situation, or some other phenomenon*” (p. 2). Descriptive research allows people who want to take part in the research study to do so.

Freitas, Bufrem, and Brenda (2016) state that the aim of explanatory research is “*to elucidate key factors for the occurrence of certain phenomena and the relationship established between the forces or aspects that surround them*” (p. 9). Explanatory research links ideas to provide a better understanding of causes and effects.

This study can be described as an exploratory research study. It makes use of a mixed method design that uses quantitative methods as well as qualitative methods to collect the primary data needed to understand the phenomenon being studied.

Creswell and Clark (2010) identify six major types of mixed method designs. In order to select a design, researchers must consider the level of interaction between the qualitative and quantitative methods to be used, decide whether priority will be given to qualitative or quantitative methods (an equal or unequal weighting), and think about the timing of these methods (concurrent, sequential, or multiphase). The six major mixed method designs are (Creswell & Plano Clark, 2010):

1. **Convergent Parallel Design:** The researcher collects qualitative and quantitative data simultaneously and gives equal priority to each. Each type of data is analysed independently, and the results of these analyses are interpreted together.
2. **Explanatory Sequential Design:** Quantitative data is collected and analysed first. Thereafter, qualitative data is collected and analysed in order to explain the quantitative results.
3. **Exploratory Sequential Design:** Qualitative data is collected and analysed first, followed by quantitative data. The two strands of data are connected afterwards.
4. **Embedded Design:** This design has a main phase during which either qualitative or quantitative data is collected. Analysis can happen before, during, or after the main phase of the design.
5. **Transformative Design:** A theoretical framework is used as a guide to collect and analyse qualitative and quantitative data concurrently or sequentially.

- 6. Multiphase Design:** This design combines the concurrent and sequential collection and analysis of qualitative and quantitative data over multiple phases within a research study.

The design chosen for this research study is the convergent parallel design. The convergent parallel design includes both a quantitative and a qualitative strand of data. Quantitative data will be collected using a survey (Chapter 3), and qualitative data will be used for the identification of best practices (Chapter 4).

The quantitative results will be analysed using descriptive statistics (section 1.7.2.1), and the qualitative results will be analysed using a qualitative content analysis (section 1.7.2.3). The convergent parallel design allows the independent execution of both strands of data with the goal of merging the quantitative and qualitative results towards the end of the study to develop a complete list of best practices.

The research process followed and the research methods used in this study are discussed in section 1.6 and section 1.7, respectively.

1.6 Research Process

According to Drew, Hardman, and Hosp (2007), a research process is “the steps involved, from investigating an idea to developing the research questions” (p. 33). It is the order in which the steps of a research investigation are performed. This process allows researchers to observe subjects and analyse data in order to answer research questions. This study’s research process is illustrated in Figure 1.1. The figure shows the main research objective, the research sub-questions, the research methods used to answer the research questions, and the research outputs. The research methods used are discussed in greater detail in section 1.7.

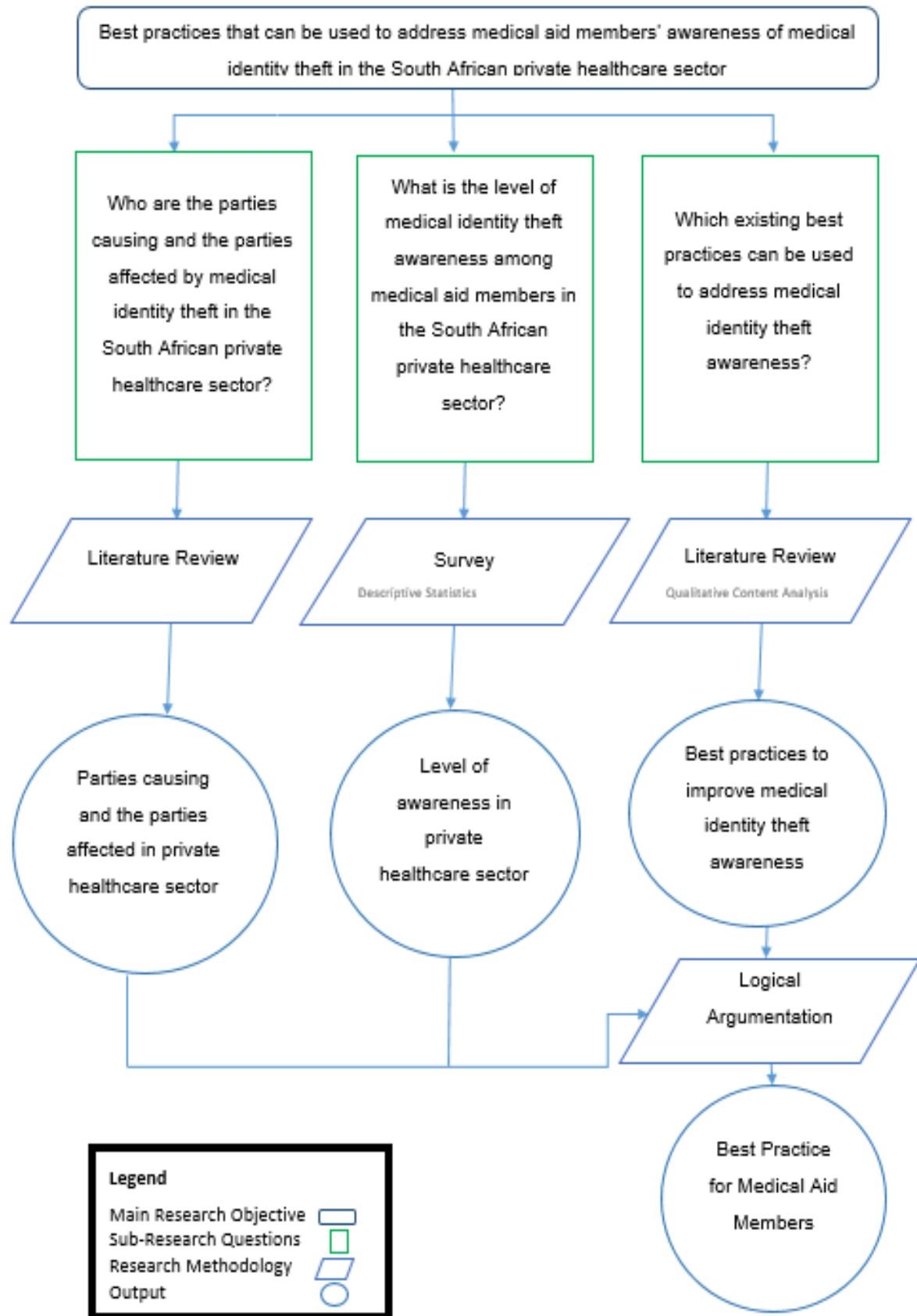


Figure 1.1: Research Process

1.7 Research Methods

Walliman (2010) defines research methods as “*the tools and techniques for doing research*” (p. 1). This research study uses a literature review, a survey, descriptive statistics, logical argumentation, and a qualitative content analysis to address the research questions. These research methods are used for data collection (section 1.7.1) and data analysis (section 1.7.2).

1.7.1 Data Collection

Goodwin et al. (2006) define data collection as “*the activity of acquiring and compiling information from different sources*” (p. 4). This research study collects data using a literature review and a survey.

1.7.1.1 Literature Review

A literature review is a comprehensive study of the literature on a topic that can be used to answer research questions (Aveyard, 2010). A literature review can make use of books, journal articles, electronic databases, government publications, and reports. This research method lays the foundation for the advancement of knowledge within specific fields of interest and can result in theory development as well as the discovery of further research areas.

In this study, a literature review is conducted to identify the parties causing and the parties affected by medical identity theft. Furthermore, a literature review is used to identify best practices for raising awareness of medical identity theft among medical aid members in the private healthcare sector.

1.7.1.2 Survey

A survey is a structured questionnaire that is administered to individuals to gather information or collect data. Surveys can be completed in person, on paper, online, or over the phone (Olivier, 2009).

Surveys can be categorized into questionnaires and interviews. A questionnaire is a research tool that uses a series of questions to gather information through computer assisted or pen-and-paper data collection (Brancato et al., 2006). An interview is a formal meeting wherein the assessor asks structured questions to ensure that as much information as possible is obtained from the respondent to address the aim and objectives of the research study (Gill, Stewart, Treasure, & Chadwick, 2008).

Chapter 1: Introduction

A survey was conducted to achieve the second sub-objective of this research study. A similar survey, sponsored by the Medical Identity Fraud Alliance (MIFA), was conducted in the United States in 2013 by the US Ponemon Institute to observe the impact of medical identity theft on consumers (US Ponemon Institute, 2013). This survey was modified to suit the purpose of this study, which was based in South Africa. The modified survey took the form of a structured questionnaire and included closed-ended and open-ended questions.

Cheung (2014) defines a structured questionnaire as “*a document that consists of a set of standardized questions with a fixed scheme, which specifies the exact wording and order of the questions, for gathering information from respondents*” (p. 273). Lavrakas (2018) defines a closed-ended question as “*one that provides respondents with a fixed number of responses from which to choose an answer*” (p. 2). Yes-no or multiple choice questions can be used to control respondents’ responses. According to Lewis-Beck, Bryman, and Futing Liao (2004), “*respondents can provide answers to open questions in their own terms or in a manner that reflects the respondents’ own perceptions rather than those of the researcher*” (p. 2). Furthermore, open-ended questions allow follow-up questions to clarify respondents’ answers.

Social networks and online surveys, such as SurveyMonkey, SurveyGizmo, or Free Online Surveys, provide a convenient means of data collection. The survey used in this study was distributed digitally in order to reach a large number of participants.

Daniel (2012) defines sampling as “*the selection of a subset of a population for inclusion in a study*” (p. 1). Sampling selects a group of people from a population to participate in a research study. There are two major types of sampling, namely probability (random) and non-probability (non-random) sampling (Taherdoost, 2016).

According to Kolb (2008), probability sampling requires the “*ability to calculate exactly the probability of a single person in a sampling frame being chosen to participate*” (p. 182). A sample that has an equal chance of being selected from the population as any other sample can act as a representative sample.

According to Lavrakas (2008), non-probability sampling “*does not attempt to select a random sample from the population of interest*” (p. 1). With non-probability sampling, the chance of an individual from the population being selected for the sample is unknown.

Chapter 1: Introduction

In this research study, non-probability sampling is used. Exploratory research identifies existing issues or problems. The current research identified the issue of South African medical aid members being affected by medical identity theft. Although non-probability sampling does not provide as good a representation of the population as probability sampling, non-probability techniques can help researchers learn more about the population (Yang, 2010). Several non-probability sampling techniques exist.

Sedgwick (2014) explains that in convenience sampling “*subjects are selected because of their convenient accessibility and proximity to the researcher*” (p. 1). Convenience sampling is a subtype of non-probability sampling wherein the participants are individuals who the researcher could easily contact for assistance.

Jupp (2018) defines volunteer sampling as being used for “*sensitive research when it is necessary to rely on those who are willing to answer requests to provide data*” (p. 2). Volunteer sampling is a subtype of non-probability sampling, as it is unknown which individuals from the population will be participating.

Johnson (2014) defines snowball sampling as “*a non-probability method of survey sample selection that is commonly used to locate rare or difficult to find populations*” (p. 1). Snowball sampling can be used with a survey by allowing participants to forward a link to the survey to other participants via email or social media, which can lead to a wide distribution scheme and a diverse set of respondents who have the required characteristics.

Patton (2014) defines purposive sampling (also known as judgement, selective, or subjective sampling) as “*[s]electing information-rich cases to study, cases that by their nature and substance will illuminate the inquiry question being investigated*” (p. 264). Purposive sampling is a subtype of non-probability sampling. Participants are selected based on the researcher’s judgement of who will have the necessary experience and be interested in participating.

Given (2008) explains that quota sampling “*uses key categories in the larger population to specify how many members of the sample should fall into each of those categories or combinations of categories*” (p. 722). Quota sampling is a subtype of non-probability sampling. It is very similar to stratified sampling, as the population is divided into groups.

For this research study, purposive sampling was used to identify participants aged 18 or older who had experience as medical aid members. Individuals who were willing to participate volunteered after receiving a request (volunteer sampling) and forwarded a link to other potential participants (snowball sampling). These sampling techniques enabled the researcher to obtain the results required to achieve the objectives of the research study.

1.7.2 Data Analysis

Coghlan and Brydon-Miller (2014a) define data analysis as “*processes associated with surfacing meaning and understanding from the various data sets that may be collected during the action research as a basis for further action and theory building*” (p. 239). The following sections discuss descriptive statistics, logical argumentation, and qualitative content analysis.

1.7.2.1 Descriptive Statistics

Descriptive statistics use calculations to summarise a given data set. A short summary describing the sample and the measures of the data is provided (Olivier, 2009). This summary combined with a simple graphical analysis provides a quantitative analysis of the data (William, 2006). Descriptive statistics express what the collected data reveals in a graphical manner.

1.7.2.2 Logical Argumentation

An argument is developed from a set of premises that lead to a conclusion through logical implications (Olivier, 2009). In this research study, logical argumentation is applied to develop best practices for addressing medical identity theft awareness in South Africa by using the results of the literature review and the survey questionnaire.

1.7.2.3 Qualitative Content Analysis

Hsieh and Shannon (2005) define qualitative content analysis as “*a research method for the subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes or patterns*” (p.1278). In this study, a qualitative content analysis is applied to the existing best practices for addressing medical aid members’ awareness of medical identity theft, which are identified using various literature sources, to produce a list of best practices for South African medical aid members.

1.8 Ethical Considerations

Ethics approval was granted by Nelson Mandela University and is attached as Annexure 1.

No confidential information was accessed or published for the purpose of this research project. Participation in the questionnaire and interviews was voluntary, and the participants will remain anonymous.

1.9 Conclusion

Chapter 1 commenced by discussing the background of the healthcare sector and progressed towards the main topic of medical identity theft. In section 1.2, the problem statement was identified. Section 1.3 determined the research objectives, and the research questions were identified in section 1.4. The research methodology was discussed and explained in section 1.5. Further insight into the research process was provided through the use of a diagram (Figure 1.1). The research methods used for data collection and data analysis were elaborated on in section 1.7.1 and section 1.7.2. The chapter concluded with ethical considerations in section 1.8. Chapter 2 will discuss the parties causing and the parties affected by medical identity theft in South Africa.

Chapter 2 **MEDICAL IDENTITY THEFT**

2.1 Introduction

In Chapter 1, the nature and purpose of medical identity theft was discussed. The aim of this chapter is to identify who is causing medical identity theft. Section 2.2 looks at the private healthcare sector and the types of role players involved therein. Thereafter, the types of medical records kept by each role player are identified. Section 2.3 explains healthcare fraud and identifies the parties possibly involved therein. The main focus of the chapter is diving deeper into medical identity theft by exploring the possible roles played by different individuals, which are explained in depth in section 2.4. This leads to the role players causing medical identity theft being identified in section 2.5. Figure 2.2 explains and outlines how these role players cause medical identity theft using the healthcare sector as a framework. The reasons the different role players have for committing medical identity theft are also summarised. Lastly, section 2.6 explains the impact medical identity theft has by using a case scenario. The consequences of medical identity theft for different role players are also summarised at the end of this section.

2.2 Private Healthcare Sector

In Chapter 1, two types of healthcare sectors (private and public) were identified. This chapter will focus on the private healthcare sector and medical aid members. The private healthcare sector has extensive connections to healthcare professionals (people) and the healthcare industry (providers), with 18% of the population being able to afford private medical aid treatment from the private healthcare sector (Expatica, 2019).

Chapter 2: Medical Identity Theft

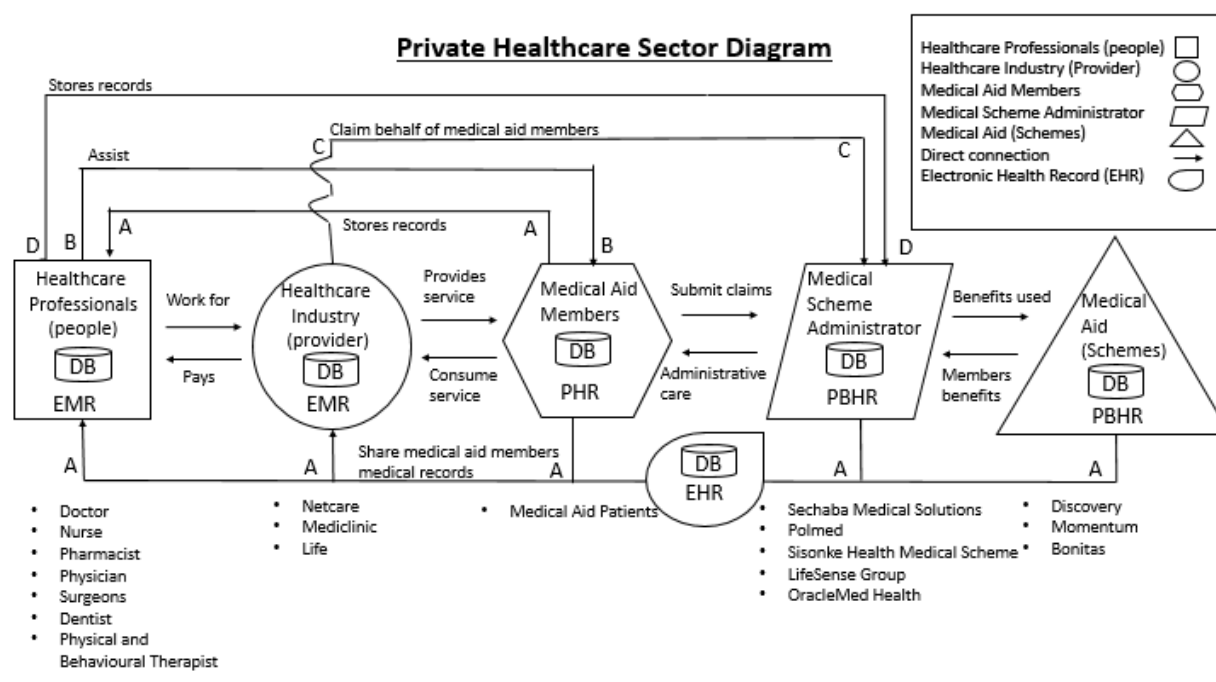


Figure 2.1: Private Healthcare Sector Diagram

The following five role players are involved in the private healthcare sector (illustrated in Figure 2.1 using various shapes):


1. Healthcare professionals
2. The healthcare industry
3. Medical aid members
4. The medical scheme administrator
5. Medical aids (schemes)


Healthcare professionals, represented by a square (□), are licensed and qualified professionals educated and trained to assist patients with medical services, who are working in the healthcare industry or privately (Skela-Savič, MacRae, Lillo-Crespo, & Rooney, 2017). Healthcare professionals are skilled and assist patients by diagnosing and treating illnesses. Examples of healthcare professionals include, but are not limited to, doctors, nurses, pharmacists, physicians, surgeons, dentists, and physical and behavioural therapists.


The healthcare industry, represented by a circle (○), consists of various medical sectors integrated into the economy, which assist in meeting the needs of a patients through medical treatment (Ledesma, Mcculloh, Wieck, & Yang, 2019). Healthcare


Chapter 2: Medical Identity Theft

industry providers allow patients to seek assistance from healthcare professionals, thereby providing medical services in the healthcare industry.

Medical aid members, represented by a hexagon (), are private medical aid members who pay a monthly fee and in return are covered for medical treatment from healthcare professionals by a medical aid (Key Health, 2019). Medical aid members contribute a monthly fee. Their membership fee is increased annually by the medical aid.

Medical scheme administrators aim to make a profit through their operations. Medical scheme administrators, represented by a parallelogram (), are financially sound third parties that ensure that medical aid are cost effective for both the medical aid members and the medical aid and handle all administrative duties (Council for medical schemes, 2010). The medical scheme administrator ensures that administrative care is provided to all medical aid members based on their medical aid and what benefits they can receive.

Medical aid are non-profit organizations that aim to meet a societal need and do not prioritize profit. Medical aid, represented by a triangle (), cover medical aid members for in-hospital treatment or chronic conditions. Members will receive sets of benefits that are managed by the medical administrative scheme based on their medical aid plan (Fedhealth, 2016). South Africa has various types of medical aids companies. Discovery, Bonitas, Momentum Health, BestMed, and MediHelp are some of the most widely recognised medical aid among the numerous that exist in South Africa (BusinessTech, 2019).

Medical records are shared and stored in databases. These are represented by the cylinders () in Figure 2.1. The types of medical records that will be explained further include the following:

- Electronic medical records (EMRs)
- Electronic health records (EHRs)
- Personal health records (PHRs)
- Payer-based health records (PBHRs).

For the purpose of this study, the focus is on medical records of medical aid members and on the private health sector.

Chapter 2: Medical Identity Theft

Electronic medical records (EMRs) are digital records of medical histories used within the healthcare industry to keep track of medical aid members' medical results and notes on their previous diagnoses and prescribed medications. These records are used by healthcare professionals when diagnosing and treating members (Kruse, Stein, Thomas, & Kaur, 2018). As shown in Figure 2.1, EMRs are used by both healthcare professionals and the healthcare industry to share medical information. They allow healthcare professionals to record, search for, and manage information. This ensures that the information used in the treatment of medical aid members is as comprehensive and accurate as possible.

An electronic health record (EHR) refers to a digital platform containing information regarding the medical history of a medical aid member that can be shared with various healthcare industries and healthcare professionals across multiple networks. The member's permission and approval is needed before the data can be shared (Evans, 2016). This provides healthcare professionals with quick and easy access to medical aid member records from other healthcare professionals. An EHR provides a member's contact information, allergies, family history, insurance information, history of previous medications, digital health record charts, and other information (Rouse, 2017). South Africa is still working towards developing EHRs; therefore, EHRs are excluded from this research (Katurura & Cilliers, 2018).

A personal health record (PHR) refers to a digital platform to which a medical aid member has access which provides an overview of their health data and information. Members can also approve healthcare professionals who are allowed to view their PHR (Lester, Boateng, Studeny, & Coustasse, 2016). PHRs help improve members' engagement in tracking their health status over time. PHRs include only limited information on members' medications, lab reports, and healthcare visits.

Payer-based health records (PBHRs) contain data collected from medical aid members, such as registration dates, premium increases, and contributions, in order for the medical aid to keep track of laboratory results, prescriptions, radiology reports, and other information (Congressional Budget Office, 2019). PBHRs provide an easy data sharing method for healthcare industries and healthcare professionals and allow medical aid members to distribute information with ease and efficiency. Two role players are involved in the management of PBHRs, namely the medical aid and the medical scheme administrator.

Chapter 2: Medical Identity Theft

In Figure 2.1, Line A indicates that data and information is being shared between all five role players. Healthcare professionals and the healthcare industry can request all existing records containing medical information about medical aid members from the medical scheme administrator and the medical aid. Furthermore, Line A also indicates medical aid members' records and information being stored by healthcare professionals. Healthcare professionals will request records from medical aid members, the medical scheme administrator, and the medical aid to obtain comprehensive medical records (medical history) for the medical aid members (Gillespie, 2012).

As represented in Figure 2.1 by Line B, healthcare professionals will assist medical aid members by using previous health record checks to gain accurate medical histories, which can assist in current diagnoses and ensure accuracy when prescribing or approving treatments based on current conditions (Fitzgerald, 2009).

In Figure 2.1, Line C indicates that the healthcare industry will claim the cost of services provided by healthcare professionals from the medical aid member's profile account through the medical scheme administrator (Rowe & Moodley, 2013).

Line D in Figure 2.1 indicates that medical aid member records are uploaded to and stored in the medical scheme administrator's database by healthcare professionals (Gray, Riddin, & Jugathpal, 2016). New and updated medical aid member data is collected and stored by healthcare professionals to create an accurate medical history.

The sharing of medical data over electronic networks, for example between healthcare professionals and medical aids (Figure 2.1, Line A), increases the risk of medical identity theft, as perpetrators can easily obtain personal data about individuals for their own use (Cavoukian, 2008). While sharing data electronically benefits the healthcare sector in terms of accessibility, efficiency, collaboration, and scalability, the threat of possible medical identity theft is always looming. Therefore, the different role players in the healthcare sector all keep their own records and keep track of information obtained from other role players that forms part of medical aid members' medical records.

In the following section, a deeper understanding of healthcare fraud is developed.

2.3 Healthcare Fraud

Healthcare fraud is described in various ways within literature. This section provides some examples as well as clarification regarding the definition used within this dissertation.

Chapter 2: Medical Identity Theft

Cornell Law School defines healthcare fraud as “*a type of white-collar crime that involves the filing of dishonest health care claims in order to turn a profit*” (Cornell Law School, 2017, p. 1). Dr David Botsko breaks down healthcare fraud as being composed of fraud, waste, and abuse (Botsko, 2019):

- **Fraud:** Fraud refers to the illegal act of knowingly submitting fraudulent claims to the medical aid (falsifying medical claims) in order to make a profit.
- **Waste:** Waste refers to the illegal act of overusing services, for example by ordering excessive diagnostic tests.
- **Abuse:** Abuse refers to making use of services or products provided by healthcare professionals in a way that creates unnecessary costs for the medical aid or for a medical aid member, for example by upcoding (charging the medical aid for more complex and expensive services or products than were actually provided).

The National Health Care Anti-Fraud Association (NHCAA) in the United States defines healthcare fraud as “an intentional deception or misrepresentation that the individual or entity makes knowing that the misrepresentation could result in some unauthorized benefit to the individual, or entity or to some other party” (National Health Care Anti-Fraud Association, 2018, p. 1).

Three parties that could possibly be involved in healthcare fraud are (Li, Huang, Jin, & Shi, 2008):

1. Healthcare professionals
2. Medical aid members
3. Medical aids.

From the previous three definitions, it can be concluded that healthcare fraud can be committed by individuals working in the healthcare industry, in healthcare professions, or for medical aids, with or without the knowledge of the medical aid members, by submitting inaccurate or false claims to medical aid to obtain profits or benefits.

Healthcare fraud is rapidly becoming the crime with the highest year-on-year growth in South Africa, currently costing the South African economy an estimated R930 million per annum (Molefe, 2018). Medical aid members' lack of knowledge and understanding allows healthcare professionals to abuse their position and obtain compensation for services that were never delivered. During tough economic times, healthcare

Chapter 2: Medical Identity Theft

professionals may make an irrational decision and commit healthcare fraud (Dean, Vazquez-Gonzalez, & Fricker, 2013).

As the cost of health care increases, healthcare fraud is becoming a greater concern, not only for the healthcare industry, but also for patients and medical aids (ENCA, 2018). According to Liou, Tang, and Chen (2008), several countries have expressed major concern about healthcare fraud and abuse, citing billions of dollars of financial losses in public and private financial institutions every year. Healthcare fraud is increasing and creating problems for all healthcare industries. It is affecting patients seeking health care and causing exorbitant expenses to be incurred by individuals (Davis, 2012).

The involvement of various role players within the healthcare sector in healthcare fraud can impact medical aid members through financial consequences or by causing data inaccuracies. The following section will aim to provide a deeper understanding of medical identity theft, one of the ways in which healthcare fraud can be committed, and the role players involved therein.

2.4 Medical Identity Theft

As mentioned in Chapter 1, identity theft is a complex topic worthy of its own dissertation. This work concentrates on identity theft in the context of the medical industry. Focus is placed on medical identity theft specifically in order to understand it more comprehensively and in greater detail. This section provides some examples of definitions of medical identity theft and clarifies which definition is used within this dissertation.

According to Pam Dixon (2006) of the World Privacy Forum, medical identity theft as *“uses a person’s name and sometimes other parts of their identity – such as insurance information – without the person’s knowledge or consent to obtain medical services or goods or uses the person’s identity information to make false claims for medical services or goods”*. She further explains that medical identity theft can lead to *“erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim’s name”* (p. 5).

Frankenfield (2018) defines medical identity theft as *“the fraudulent use of a person’s health insurance information to receive reimbursement for health care services provided to an individual not covered by the policy”* (p. 1).

Chapter 2: Medical Identity Theft

Webb (Webb, 2007) defines medical identity theft as “*where a person uses another person’s identity without consent, in order to obtain medical treatment services or therapeutic goods they are not authorised to receive*” (p. 217).

Medical identity theft is committed by hackers and fraudsters. The definitions of these terms that are used within this dissertation will now be explained in greater detail.

Rouse (2019) defines a **hacker** as an “*individual who uses computer, networking or other skills to overcome a technical problem*” (p. 1). There are several types of hackers, and they can be good (white hats) or bad (black hats). Looking specifically at black hats, Andress and Winterfeld (2014) describe a black hat hacker as a skilled individual with an in-depth knowledge of computers who is able to attack and exploit vulnerabilities within a network or computer system

In the context of medical identity theft, hackers can be defined as individuals skilled in cyber technology who intend to gain access to the healthcare sector’s network to search for vulnerable medical aid members’ personal information.

Fraudsters are individuals who commit illegal acts of fraud (for example. scams) for benefits or profit (Orton-Jones, 2017). These fraudsters can commit internal or external fraud.

According to the Association of Certified Fraud Examiners (2019), **internal fraud** (also known as occupational fraud) can be defined as “*the use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the organization’s resources or assets*” (p. 1).

According to Phua et al. (1998), **external fraudsters** can be defined as “*individual criminal offenders and organised/group crime offenders (professional/career fraudsters) because they repeatedly disguise their true identities and/or evolve their modus operandi over time to approximate legal forms and to counter detection systems*” (p. 2).

In the context of medical identity theft, internal and external fraud can be defined as any dishonest action caused by internal or external role players, respectively. The four role players referenced in Figure 2.1 (healthcare professionals, the healthcare industry, the medical scheme administrator, and the medical aid) can be seen as internal fraudsters who use their skills and management levels (abuse their power as leaders) to bend rules for personal gain. Action taken with medical aid members’ involvement (collusion) is seen not as medical identity theft but as fraud committed by these role players. External

Chapter 2: Medical Identity Theft

fraudsters are individuals who attempt to acquire medical treatment by illegally purchasing stolen medical aid member information from hackers.

Based on the aforementioned definitions, medical identity theft can be defined as when a hacker or internal fraudster steals medical data from the healthcare sector and either sells it to external fraudsters known as perpetrators or uses it to obtain medical services or goods through impersonation. Throughout this dissertation, the terms internal fraudster and external fraudster are used, and in certain cases, the terms hacker and perpetrator are used to specify the type of external fraudster.

External fraudsters (specifically hackers) target medical records, as they contain more information than credit records and this type of information is worth more than others on dark sites (Schaffer, 2018). The stolen data can cause exorbitant expenses for the healthcare industry and medical aids.

As the prevalence of medical identity theft is continuously growing, medical aid members need to be aware of the parties that cause and the parties that are affected by medical identity theft. Medical identity theft is made particularly complex by the number of role players within the system. Table 2.1 presents the different role players involved in committing medical identity theft.

Table 2.1: *Role Players Involved in Committing Medical Identity Theft*

Internal Fraudsters	External Fraudsters
<ul style="list-style-type: none">• Healthcare professionals• Healthcare industry providers• Medical scheme administrators• Medical aids (schemes)	<ul style="list-style-type: none">• Hackers• perpetrators

This description does not include possible collusion between some role players. Actions taken with the involvement of medical aid members are not seen as medical identity theft, but rather as fraud. In the case of medical identity theft, medical aid members may not even be aware that their medical identities have been stolen (Molefe, 2018).

Expenses caused by medical identity theft are the responsibility of the healthcare provider. Any changes to the medical aid member records must be rectified and reimbursements need to be covered by the healthcare provider (Stowell, Schmidt, & Wadlinger, 2018). Amending incorrect medical information is not the medical aid

Chapter 2: Medical Identity Theft

member's responsibility. The healthcare provider is responsible for verifying the identity of the patient to ensure that they really are a medical aid member. Therefore, the healthcare provider will be held liable for any incorrect information and any expenses caused by medical identity theft.

Medical identity theft can have serious lingering effects on patients and the healthcare industry. Having personal data, such as information on medical tests, diagnoses, and procedures, lost or stolen due to a lack of integrity can significantly affect future healthcare services provided by medical aid organizations (Security News, 2016). Patients become aware that they are victims of medical identity theft only once they receive a fraudulent bill or notice a discrepancy in their accounts when they are charged for a service or medication which they never received (US Ponemon Institute, 2013). The following section will explain who is causing medical identity theft within the healthcare sector.

2.5 Who Is Causing Medical Identity Theft?

Medical identity theft is caused by the deceitful role players (internal and external fraudsters) identified in the section 2.4, who gain unlawful access to patients' medical data for personal gain (Thornton, Brinkhuis, Amrit, & Aly, 2015). Figure 2.2 expands on Figure 2.1 by incorporating the role players identified in section 2.4.

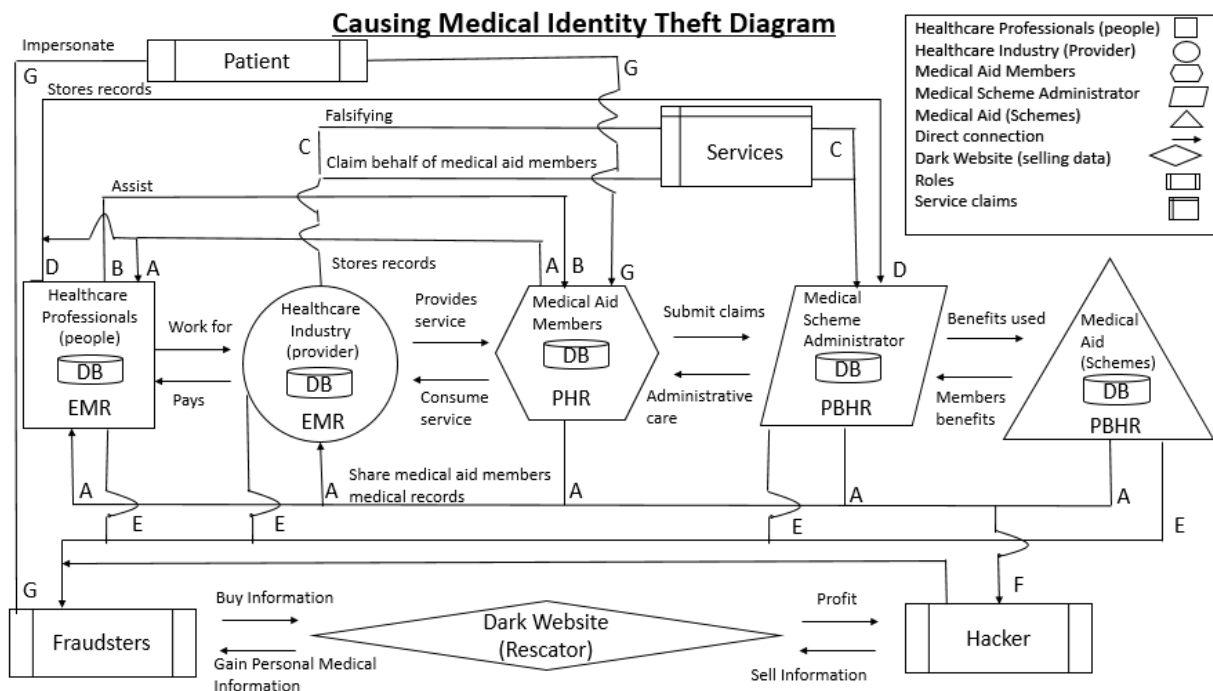



Figure 2.2: Role Players Causing Medical Identity Theft


Chapter 2: Medical Identity Theft

Figure 2.2 illustrates how the actions of the role players involved in medical identity theft (internal and external fraudsters) lead to medical data being stolen. Fraudsters can use this medical data for financial gain or to obtain medical treatments or goods. The diagram will now be described and explained in greater detail.

Line A indicates medical aid members' medical information being distributed across the network. The medical aid, medical scheme administrator, medical aid members, healthcare industry, and healthcare professionals in the healthcare sector all have access to this information. This allows any knowledgeable role player to take advantage thereof to commit internal fraud.

Line F indicates hackers finding a weakness to use as an access point into the healthcare sector's network (Line A), as discussed in section 2.4. Once an external fraudster has acquired personal information from the medical aid's database, their intention may be to sell the medical aid members' details to other external fraudulent individuals on dark websites to make a profit or to use the details to obtain medical treatment.

Line G indicates fraudsters (internal or external) attempting to use medical aid member information. A stretched diamond () is used to represent external fraudsters buying information from dark websites in order to impersonate a patient and receive healthcare services paid for by the real patient's medical aid. Internal fraudsters have direct access to personal medical information, which they use to submit rogue claims. These rogue claims result in data entries in various databases that corrupt the medical identity and records of the victim.

The predefined process symbol () represents a fraudster impersonating a medical aid member to receive medical treatment from healthcare professionals. Line G indicates the actions of this fake patient. Line B indicates a healthcare professional assisting a patient, who could be a fraudster impersonating a medical aid member to receive medical treatment.

Therefore, the role players causing medical identity theft are hackers, perpetrators, and internal fraudsters. These role players will be discussed individually in sections 2.5.1 to 2.5.3.

2.5.1 External Fraudsters: Hackers

The digital age is progressing and necessitates the digital storage of records in secured databases. However, digitalization creates opportunities for data breaches, which could be caused by negligence or by the malicious actions of hackers (Stocks, 2019). A recent interview by Anna Werner of CBS News, which was published both as an article and as a video interview, details the struggles of a victim, Brandon, with medical identity theft (CBS This Morning, 2019; Werner, 2019). Further investigation by Werner helped her to understand how easy medical identity theft can be for hackers and with what intentions they steal medical data from the healthcare sector. A cybersecurity expert, Gary Miliefsky, was able to obtain medical information and records from the dark web within three seconds. He identified another hacker selling children's health records labelled "USA KIDS FULLZ" as well as many other incidents of hackers trying to sell medical information to make a profit.

Another tool used by hackers is ransomware. In 2019, multiple hospital systems belonging to Hackensack Meridian Health in New Jersey were attacked by ransomware and taken over by hackers. This left the healthcare system vulnerable, as all staff members were locked out of and had no control over the hospital systems (Cohen, 2019). The hackers encrypted these systems, leaving the healthcare providers with no choice but to pay the ransom demand so that the systems could be decrypted and business could continue.

According to D'Alfonso (2015), there is a high demand for medical aid identity profiles on the black market, making them a valuable commodity on underground websites such as Rescator. Hackers take advantage of opportunities to gain access to personal information and commit medical identity theft. They are aware that the healthcare sector has poor infrastructure and lacks individuals skilled in IT who can adequately secure data.

Numerous cases of medical identity theft have been reported. Dietsche (2018) reported on a survey created by the software company Nuix to determine how easy it would be for hackers to access the healthcare sector. The survey could be completed anonymously online or in person during a Nuix conference, and 112 hackers completed it (Dietsche, 2018). The responses obtained showed that the hackers saw the healthcare sector as an easy target with weak security. It was found that 38% of the

participants could easily obtain personal medical aid information within an hour and sell this data on the dark web.

Therefore, the main benefit of hackers' illegal activities is financial gain. Hackers also keep the personal medical aid information for further use, which is another benefit (Carroll, 2019). This creates a continuous risk for medical aid members, as their medical information is available to potential hackers. In the following section, the ways in which perpetrators cause medical identity theft will be discussed.

2.5.2 External Fraudsters: Perpetrators

As explained in section 2.4 and depicted in Figure 2.2, fraudsters use victims' medical aid member information, which can easily be purchased over the dark web, as personal information to obtain health services (Mancini, 2014). The following two types of fraudsters each play a role in medical identity theft:

1. Perpetrators – Perpetrators purchase stolen medical aid information from illegal sites and use it to obtain medical care and services.
2. Hackers – Hackers use medical aid information stolen from the healthcare sector to obtain personal healthcare treatments.

Perpetrators obtain medical aid member information from hackers who sell it on dark websites, as mentioned in section 2.5. Thus, such information is available to any member of the public who is willing to purchase it. Such an individual can use a medical aid member's personally identifiable information and assume their identity to receive medical treatment or drugs. Various such cases exist. For example, a Pennsylvania man found out that his medical identity was used at five different hospitals. The perpetrator received services worth over \$100,000 and left behind false medical results in the victim's name (Stateline, 2014). In this case, a fraudster impersonated a medical aid member to obtain medical services. Using the dark web, this perpetrator was able to find a vulnerable medical aid member in his area and assume his identity to obtain medical assistance for the price the hacker charged for the medical information. Medical aids can be extremely expensive, leaving perpetrators to resort to illegal activities to receive medical care.

The possible benefits of medical identity theft for fraudsters include financial gain as well as medical aid benefits in the form of prescription drugs or treatments (Fraud Org,

1996). In the following section, the ways in which internal fraudsters cause medical identity theft will be discussed.

2.5.3 Internal Fraudsters

As explained in section 2.4, internal fraudsters are members of the healthcare sector who sell patients' medical aid information for personal gain. Internal fraudsters are often very difficult to catch due to their innate understanding of the systems they are fraudulently using. Furthermore, their fraud practices are often relatively small and innocuous (Molefe, 2018). This type of medical identity theft may entail exposing victims' details to make a profit or stealing them to give to other patients the insider knows and wants to help (University of Miami Miller School of Medicine, 2019). Regardless of their severity, such instances of medical identity theft lead to victims' personally identifiable information being exposed. Similarly to external fraud, internal fraud can have detrimental effects on both the victims and their medical aids by causing data inaccuracies. Owing to their insider status, healthcare professionals can commit medical identity theft in several unique ways (Molefe, 2018), including:

1. using the details of patients covered by medical aids when treating other people
2. claiming for services that were not provided on behalf of patients

According to Frankenfield (2018), the reasons healthcare professionals steal medical aid members' personal information include financial gain, revenge, and other agendas. A medical aid member reported to their medical aid that a dietician used their membership information to claim compensation for services that were not rendered. Upon further investigation, the medical aid discovered multiple false claims made by the dietician (Molefe, 2018).

In 2017, an article by MoneyMarketing (2017) titled "Fighting fraud in the healthcare industry" reported that three fake medical technologists in Limpopo collaborated with medical doctors and were found guilty of committing medical identity theft numerous times over a 10-year period. The main instances of medical identity theft resulted in claims for unnecessary tests being made to the Bonitas Medical Fund medical aid, costing over R1.3 million (MoneyMarketing, 2017).

These are only two examples of the many types of internal fraud committed by trusted healthcare sector employees for their own personal gain. As internal fraudsters have a

Chapter 2: Medical Identity Theft

deep knowledge of the procedures and the operations involved in claims, committing internal fraud is easier for staff members than for outsiders.

Monetary gain is the primary incentive to commit the majority of these crimes. An internal fraudster may act individually or with the help of other fraudulent insiders. Medical identity theft can result in serious penalties and consequences for healthcare professionals, the healthcare industry, medical scheme administrators, and medical aid. The following section will provide a summary of the role players causing medical identity theft.

2.5.4 Summary of the Role Players Causing Medical identity Theft

Table 2.2 provides a summary of section 2.5. It identifies the role players involved in medical identity theft as well as the reasons for their involvement while separating internal and external fraudsters.

Table 2.2: Summary of the Role Players Causing Medical Identity Theft

	Internal Fraudsters	External Fraudsters	
Role Players Causing Medical Identity Theft	<ul style="list-style-type: none"> • Healthcare professionals • The healthcare industry • Medical scheme administrators • Medical aids 	Hackers	Perpetrators
Reasons	<ul style="list-style-type: none"> • Financial gain • Claiming for services not provided • Selling medical aid patients' information to other fraudsters 	<ul style="list-style-type: none"> • Financial gain • Free medical treatment • Easily obtainable medical data • Vulnerable data 	<ul style="list-style-type: none"> • Financial gain • Free medical treatment • Easily obtainable medical data

	Internal Fraudsters	External Fraudsters	
		<ul style="list-style-type: none"> • Weak IT security in the healthcare sector • High demand and large profits 	

Table 2.2 provides a summary of the role players causing medical identity theft. Some similarities and differences between internal and external fraudsters’ reasons for committing fraud can be identified.

Internal and external fraudsters’ reasons for committing fraud are similar in that medical identity theft can lead to financial gain for all the role players.

In terms of the differences by reasons, hackers identify weak IT security within the healthcare sector in order to gain vulnerable data and being aware that there is high demand and large profit for medical identities. Perpetrators focus on obtaining medical aid information from dark websites, while internal fraudsters falsify claims or provide medical aid members’ information to other fraudsters.

The following section will explain the consequences of medical identity theft by using a case scenario from within the healthcare sector.

2.6 Consequences of Medical Identity Theft

In 2012, the economic impact of medical identity theft in the United States was estimated at \$40 billion and affected approximately 1.85 million people, including medical aid members and individuals working in the healthcare industry (Mohan, 2014). Figure 2.3 presents an in-depth diagram building on the diagram in Figure 2.2. This is followed by a case scenario illustrating the process and the consequences of medical identity theft.

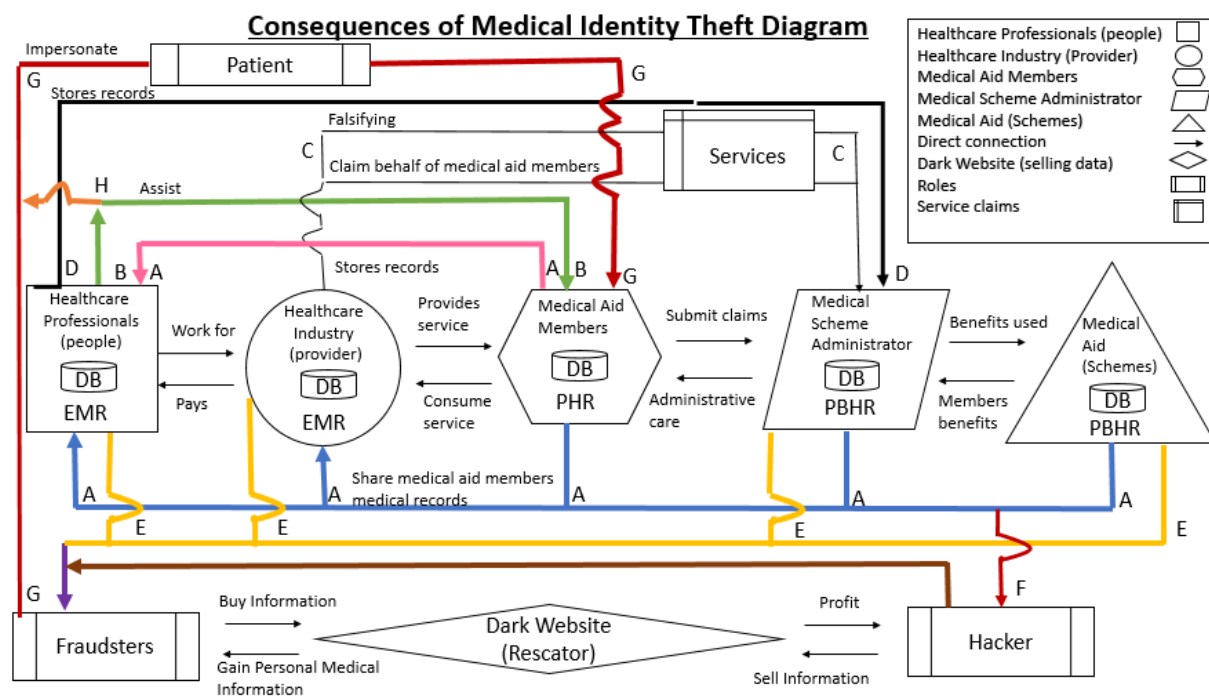


Figure 2.3: Consequences of Medical Identity Theft

Case Scenario 1: Blood transfusion incident caused by medical identity theft

Max is a 50-year-old male who has been a member of the Discovery Health Medical Scheme for over 20 years and is in very good health. Max and his wife, Martha, live in Johannesburg about 8 km away from the nearest hospital. He goes to the gym every weekday; however, he never goes to the doctor for check-ups.

Michael a 44-year-old male who has recently been struggling financially and is about to be evicted from his home due to late payments. He lives in the same area as Max and his family. Michael been sick for a few months. He believes he has cancer and the medical treatment he will need is out of his budget. His friend Tim recommended that he look at a website called Rescator. On this website, he will be able to request and buy a medical aid member's identity, which he will then be able to use to receive medical treatment.

After speaking with Tim, Michael decided to visit the Rescator website. He posted a request for a medical aid member's identity belonging to a male patient between 40 and 50 years old living in Johannesburg, South Africa. A few days later, he checked the website again, and he saw that someone was selling a medical aid member's identity with all the details he needed for R5,000.

Chapter 2: Medical Identity Theft

Michael decided to act quickly and contact the person selling the information. He made contact with the anonymous seller online. Michael did not really care who was selling the information to him. He quickly transferred the money to the anonymous bank account and waited. He was informed that he would be emailed all the relative information and receive a copy of the medical aid card in the mail once the payment had been received.

Michael, acting as the perpetrator, requests and buys personal medical information from Rescator (represented by an arrow pointing from the fraudsters to the dark website).

A few day later, Michael received a medical aid card and the membership number of a Discovery medical aid member named Max. He immediately left the house and went to the nearest hospital. He was slightly nervous, but he walked into the hospital and presented the medical aid card to the receptionist, Jill. She asked him to wait and said that the next available doctor would assist him.

*Michael receives the personal medical information from the dark website (represented by an arrow pointing from the dark website to the fraudsters).
Line G (red) indicates Michael impersonating the real medical aid member.*

Michael was relieved. A few minutes passed before a doctor called for Max. Michael quickly realised that this was the name of the medical aid member whose identity he was using and went with the doctor. Michael informed the doctor that based on the symptoms he was displaying he believed he had cancer. The doctor ran some blood tests and checks, which confirmed that Michael had stage 2 cancer. The doctor informed Michael that there was an issue with his blood type, as it was previously documented as being A-, but the blood tests now indicated that it was AB+.

*Line A (blue) indicates the healthcare professional attending to Michael requesting medical information in order to learn about the patient's history.
Line B (green) indicates the healthcare professional assisting the patient. Line H (orange) indicates that he is actually assisting an impersonator. The healthcare professional assists and diagnoses the patient believing he is the medical aid member because the receptionist approved the patient.*

Chapter 2: Medical Identity Theft

The doctor said that it was possible that the blood type listed had been entered inaccurately, as Max had hardly been to the doctor in the last 15 years. Michael was told that a few documents needed to be signed to update his blood type and to verify his identity. The doctor also informed Michael that he needed to upload his latest information in order for the medical aid and the hospital to make changes and updates.

Line A (pink) indicates the new medical data being stored by the healthcare professional, which causes inaccuracies in the hospital's medical records. Line D (black) indicates the data being sent to the medical scheme administrator to update the medical aid member's medical information, which also leads to inaccurate medical records.

Michael was concerned at first, but after this process he received a schedule for his cancer treatments and a prescription for a list of medications. He went to the pharmacist and presented the medical aid card. His medications were fully covered by the medical aid. He had managed to use Max's medical aid membership successfully and planned to use it again for his next check-up.

On a rainy weekend, Max was in a serious car accident and was immediately admitted to the nearest hospital. He lost a lot of blood due to the accident. His family was notified and called the hospital to which Max was admitted. He went into surgery and required a blood transfusion. Within minutes his body went into shock; he started getting sick and his immune system began shutting down. The doctors believed that his blood type was AB+, as this was what was indicated in his medical records.

Line A (blue) indicates Max's medical records being retrieved from various role players. Line B (green) indicates medical care being provided by healthcare professionals to a medical aid member.

A few minutes later the doctors informed Martha that her husband was in recovery but that an incident had occurred. The doctors were able to fix the issues caused by the inaccurate information regarding his blood type. However, they believed that Max's medical identity was stolen and that the perpetrator was using his medical aid information.

Max and his family are now facing financial issues, as resolving the problems caused by the medical identity theft will be expensive. They are also unaware of whether their

Chapter 2: Medical Identity Theft

medical aid savings or medical care benefits have been used up. The hospital is left with the financial repercussions of outstanding fees. As Max did not have any medical issues, Discovery will not cover expenses for services that were not provided to the correct patient. The doctor and the hospital have agreed to investigate the history of Max's medical records in order to find out what happened and prevent it from happening again.

The medical aid member is left with the daunting task of claiming back his medical identity, as the healthcare industry and his medical aid have blacklisted him.

Max's hospital will have to complete an in-depth investigation into the history of his visits and provide a list of financial expenses to the medical aid. Depending on the severity of the case, this could cost over R3,000. This leaves Max in a challenging situation, as he will be unable to receive further medical care due to his medical records being corrupted by inaccurate data and his medical aid blacklisting him until the issue is resolved.

The healthcare industry will refuse to provide medical services to the medical aid member, as he currently has outstanding medical fees. There will also be financial repercussions for the healthcare industry, as the medical aid member's credentials were not checked. The healthcare industry will spend an exorbitant amount of money on data recovery to ensure that the integrity and availability of their data is restored and that their reputation is not lost due to the medical identity theft. The medical aid member is burdened with financial issues, as expensive legal services may be required to resolve this situation and recover his identity.

The following section will summarise the consequences of medical identity theft.

2.6.1 Summary of the Consequences of Medical Identity Theft

Table 2.3 provides a summary of section 2.6. It identifies the role players affected by and the consequences of medical identity theft.

Chapter 2: Medical Identity Theft

Table 2.3: Summary of the Consequences of Medical Identity Theft

Role Players Affected by Medical Identity Theft	Medical aid members	The healthcare industry and medical aids
Consequences of Medical Identity Theft	<ul style="list-style-type: none">• Inaccurate medical data• Misdiagnoses and incorrect treatments (e.g. incorrect blood type used)• Financial issues• Expensive legal services• Being blacklisted	<ul style="list-style-type: none">• Inaccurate data in healthcare industry and medical aid records• Financial repercussions• Data recovery incidents

Table 2.3 provides a summary of the consequences of medical identity theft. Some similarities and differences between the consequences of medical identity theft for medical aid members, the healthcare industry, and medical aids can be identified.

The consequences that are similar for medical aid members, healthcare professionals, and medical aids include inaccurate medical data and financial problems.

There are also some differences between the consequences for these role players. Medical aid members are negatively affected by medical data, leading to misdiagnosis and incorrect treatment. They are influenced financially, as they need to pay for legal services to recover their medical identities. Medical aid members can also be blacklisted by the healthcare industry and their medical aids, which may result in an inability to receive medical treatment and care. The healthcare industry and medical aids face financial repercussions, as they must pay for data recovery to identify and correct inaccuracies in the medical records of the victims.

In the following section, Chapter 2 will be concluded.

2.7 Conclusion

Chapter 2 commenced by discussing the private healthcare sector, the role players involved therein, and the types of records kept by each role player. Healthcare fraud was elaborated upon, and it was shown that medical identity theft is a type of fraud. In

Chapter 2: Medical Identity Theft

section 2.5, the role players causing medical identity theft were identified. Table 2.2 identified the reasons internal and external fraudsters commit medical identity theft. Section 2.6 presented a case scenario to illustrate who is affected by medical identity theft, and the consequences thereof were summarised in Table 2.3.

As the prevalence of medical identity theft is increasing, medical aid members should be made aware of these issues. According to Eva Velasquez, president and CEO of the Identity Theft Resource Center, medical identity theft is under-reported and not fully understood by victims (Grant & Young, 2016). Chapter 3 will discuss the levels of medical identity theft awareness in South Africa by referring to data gathered via a survey questionnaire completed by South Africans who previously were or currently are members of medical aids.

Chapter 3 LEVEL OF AWARENESS IN THE PRIVATE HEALTHCARE SECTOR

3.1 Introduction

In Chapter 3 a series of questions are constructed, distributed and analysed using descriptive statistics to determine the medical identity theft awareness of the respondents participating in this survey. The primary data collection process, as well as the results are thoroughly reviewed in detail. The questionnaire design and its distribution are reviewed in section 3.2. Using an exploratory mixed-method strategy (both quantitative and qualitative), primary data collected is examined to produce descriptive statistics as previously mentioned in Chapter 1. The results from the questionnaire survey are produced by means of graphs and charts for each question from section 3.3 to section 3.7. Finally, a summary is provided of each section of the questionnaire to produce a list of themes further detailed in section 3.8.

3.2 Data Collection

3.2.1 Questionnaire Design

The survey was adapted from the US Ponemon Institute, and modified for the purpose of this study based in South Africa, as mentioned in Chapter 1. Figure 3.1 shows a representation of the sections of the survey used in this questionnaire. The structural order of the questionnaire design sections has been altered, this differing from the original of the US Ponemon Institute. The survey started with the Background, Healthcare Provider Privacy, Medical Aid Privacy, Medical Identity Theft Experience and Demographics. Therefore the numbering of the questions of the current SA survey differs slightly from that of the US Ponemon Institute survey. The current survey as shown in Figure 3.1 identifies the demographic details first, followed by the remainder of the sections. This allows for a more precise sorting of the data to determine whether the respondents should continue further with the survey or not. Their participation would be terminated if all the requirements have not been met.

Chapter 3: Level of Awareness in the Private Healthcare Sector

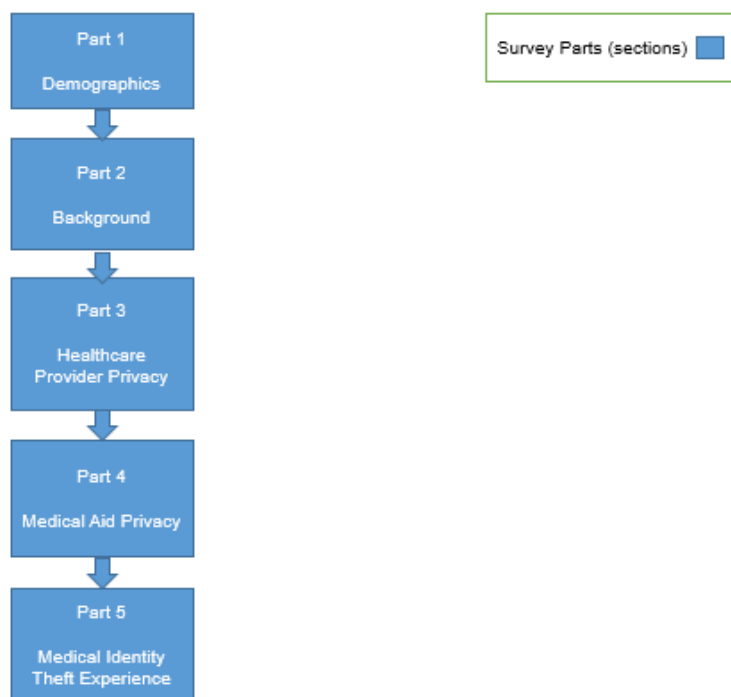


Figure 3.1: Survey Sections Parts

Questions removed from the current SA survey were those determining the highest level of education attained, the respondents' employment status and the approximate total household income earned. The questions were removed because they were not required in order to achieve the objective in this research.

Questions modified were the US geolocations to meet with SA geolocations criteria (question D2), changing the currency from \$ to R (question 22A, 22B and 22C) and identifying whether a respondent is currently or was previously a medical aid member (question D4). The US Ponemon Institute's questions to identify the health plan were focused on the US medical aids (providing several types of medical aid such as Medicare, the Government, a health savings plan, or private insurance) whereas in the current survey, the questions have been modified to identify whether a respondent is currently or was previously a member of medical aid and if so, which medical aid they were a member of. In question Q2 another option field has been added, namely 'Other (please specify)', allowing respondents to give their own responses on how they had learnt about medical identity theft. The US Ponemon Institute survey terminology has thus been altered throughout the survey in accordance with SA terminology, as mentioned in Chapter 1.

Question added to the current survey in SA include listing any issues or comments the respondents (Question Q25) may have about medical identity theft. This enabled qualitative information to be obtained from the respondents.

Part 1 of the Demographics allows for the elimination of non-eligible respondents by identifying the age range and whether the respondent is currently or was previously a member of medical aid. If the age was below 18, and if the respondent was not a current or previous medical aid member, the survey would be terminated and any further progress prevented.

The majority of the questions are closed-ended questions while the rest of the questions are open-ended. The questionnaire consists of five parts as represented in Figure 3.1, each with several questions that link to various continuing questions. However, if the responses are invalid, the respondent is terminated (example: On question D4: 'Are, or have you ever been, a member of a member of medical aid?' If the respondent answered 'Not a member of Medical Aid', the respondent is terminated). The majority of the questions are required to be answered, while respondents are prevented from continuing to the next page if the questions have not been completed.

3.2.2 Questionnaire Distribution

The questionnaire was designed on Questionpro and sponsored by Nelson Mandela University. It allows for easy distribution via email or a shared website link to allow all users to complete the questionnaire via the Internet when convenient. The questions that form part of the questionnaire are discussed below in sections 3.3 to 3.7. This online survey was distributed over social media such as Facebook, LinkedIn, Mybroadband forum and The Forum SA. The survey was distributed in November 2019, and shared via all the social media. A follow-up was sent again weekly via various social media platforms and forums. On 28 May 2020, the survey ended, with the current low response rate attributed to the nature of the respondents' time and professions in terms of participation in the survey.

3.2.3 Sampling and Respondents

As previously mentioned in Chapter 1, the focus is of an exploratory nature. Therefore, having a small sample size of respondents is deemed to be adequate (Daniel, 2012). The subject of medical identity theft has not been previously studied or thoroughly researched in South Africa, as there are limited literature review leading to unsuccessful

Chapter 3: Level of Awareness in the Private Healthcare Sector

searches. A non-probability sampling technique, was used, employing three sampling methods, namely purposive sampling, volunteer sampling and snowball sampling.

A purposive sampling method is used in order to identify participants who are 18 years old or older and who have experience of being a medical aid member.

The use of a volunteer sampling method is targeted at respondents willing to participate in the research. The use of volunteer sampling cannot be generalized for the larger population, although it can reveal information about the respondents' experience with medical identity theft.

The use of snowball sampling allows respondents who participate and complete the survey to share the survey with other respondents such as friends and family members who may have an interest in the topic.

At the outset of the survey, a letter of informed consent is sent to the respondents, outlining the objective of the study and the criteria. The informed consent is attached in APPENDIX 2 – Informed Consent.

The survey questionnaire requirement criteria are the following:

- Respondent should be over 18 years old.
- They should currently be, or have previously been, a member of a medical aid.

A total of 216 respondents started the survey. Figure 3.2 further illustrates the termination of respondents and the respondents who started but did not complete the survey.

Chapter 3: Level of Awareness in the Private Healthcare Sector

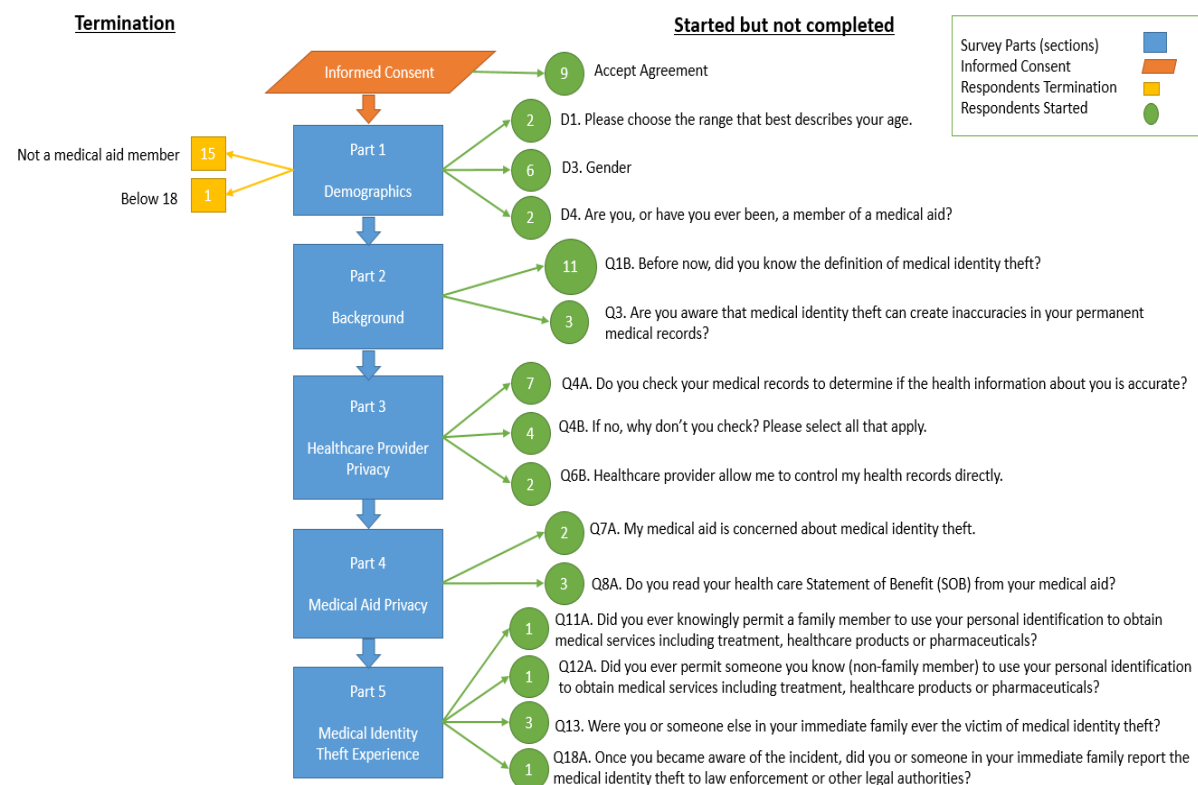


Figure 3.2: Excluded Respondents

If the criteria were not met as mentioned above, respondents were terminated as represented in Figure 3.2. The termination (left-hand side) shows the number of respondents (in yellow) who did not meet the criteria. The results are as followed:

- 15 respondents are not a medical aid member.
- One (1) respondent is under 18 years of age.

Therefore, as shown in to Figure 3.2, a total of 16 respondents were terminated for not meeting the criteria of the survey.

Figure 3.2 depicts those who started but did not complete the survey (right-hand side). It starts with the number of respondents that dropped out (in green) associated with the relevant part of the survey, then follows a letter and a number (example, D1.) and the related question. The results are as follows:

- 9 respondents dropped out in the informed consent page after the Accept Agreement.
- 2 respondents dropped out in Part 1 of question D1.
- 6 respondents dropped out in Part 1 of question D3.
- 2 respondents dropped out in Part 1 of question D4.

Chapter 3: Level of Awareness in the Private Healthcare Sector

- 11 respondents dropped out in Part 2 of question Q1B.
- 3 respondents dropped out in Part 2 of question Q3.
- 7 respondents dropped out in Part 3 of question Q4A.
- 4 respondents dropped out in Part 3 of question Q4B.
- 2 respondents dropped out in Part 3 of question Q6B.
- 2 respondents dropped out in Part 4 of question Q7A.
- 3 respondents dropped out in Part 4 of question Q8A.
- 1 respondent dropped out in Part 5 of question Q11A.
- 1 respondent dropped out in Part 5 of question Q12A.
- 3 respondents dropped out in Part 5 of question Q13.
- 1 respondent dropped out in Part 5 of question Q18A.

Therefore, 57 respondents started but did not complete the survey, thereby dropping out from participation from the survey.

Of the initial total of 216 respondents, 73 did not complete the survey. Therefore, the final number of respondents that completed the survey is 143.

In the US Ponemon Institute survey, as mentioned in Chapter 1, a total of 788 respondents who were over 18 years old participated. The respondents admitted that they or their close family members had been victims of medical identity theft (US Ponemon Institute, 2013).

In the 2013 US Ponemon survey, the 788 respondents indicated the following:

- 42% respondents have medical aid.
- 24% respondents are registered with Medicare or Medicaid.
- 21% respondents are uninsured.
- The remainder are reliant on the government, co-op plans or health savings accounts.

The US Ponemon Institute had a sample frame of 43 778 participants from all over the United States. These participants were pre-selected based on their experience with identity theft and medical identity theft. A total of 901 respondents participated in the survey. After eliminating 111 respondents who started but did not complete the survey, a final sample of 790 respondents or a response rate of 1.8% was recorded. A usable sample of 788 respondents completed the survey.

Chapter 3: Level of Awareness in the Private Healthcare Sector

Medical identity theft in the US showed a base rate of .0082, as mentioned in Chapter 1. This result was from a second independent survey sampling. To determine the US consumers' status, a discovery sampling method was used with a representative panel of adults over 18 years old who had been victims of medical identity theft. This was to determine the base rate increase over the years. The collection included 41 genuine respondents out of 5000 individuals.

The next sections (3.3 – 3.7) of the chapter present the primary data gathered from this study. Note that text formatted in italics indicates verbatim quotes from the free text-fields in the questionnaire. Section 3.3, part 1 describes the demographics of participants in the South African survey, and consists of graphs, descriptive statistics and verbatim quotes. Sections 3.4 to 3.7 each consist of four parts, namely graphs, descriptive statistics, usable verbatim quotes and discussions of the South African survey. In some sections of the qualitative data, the verbatim quotes (from Question 25) that are usable have been moved to the section (Question 1A, 2, 20B, and 21B) directly related to the verbatim quote.

3.3 Results Part 1 – Demographics

The first section summarises the biographical information of the respondents.

3.3.1 Age

As shown in Figure 3.3, the majority of the respondents were between 26 years and 35 years old. There were no participants below 18 years old. A total of 143 respondents participated in the survey.

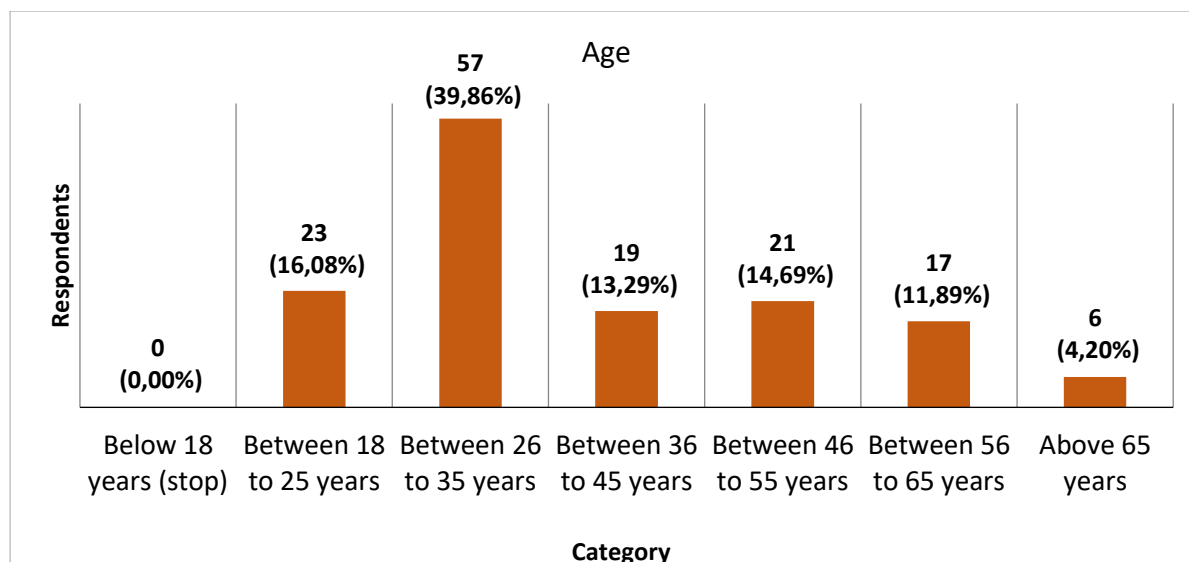


Figure 3.3: Age

3.3.2 Geographical province

Figure 3.4 shows the results of the respondents' geographical location within South Africa. It also displays the number of respondents above the percentage total, which shows a leader line to the pie chart illustration.

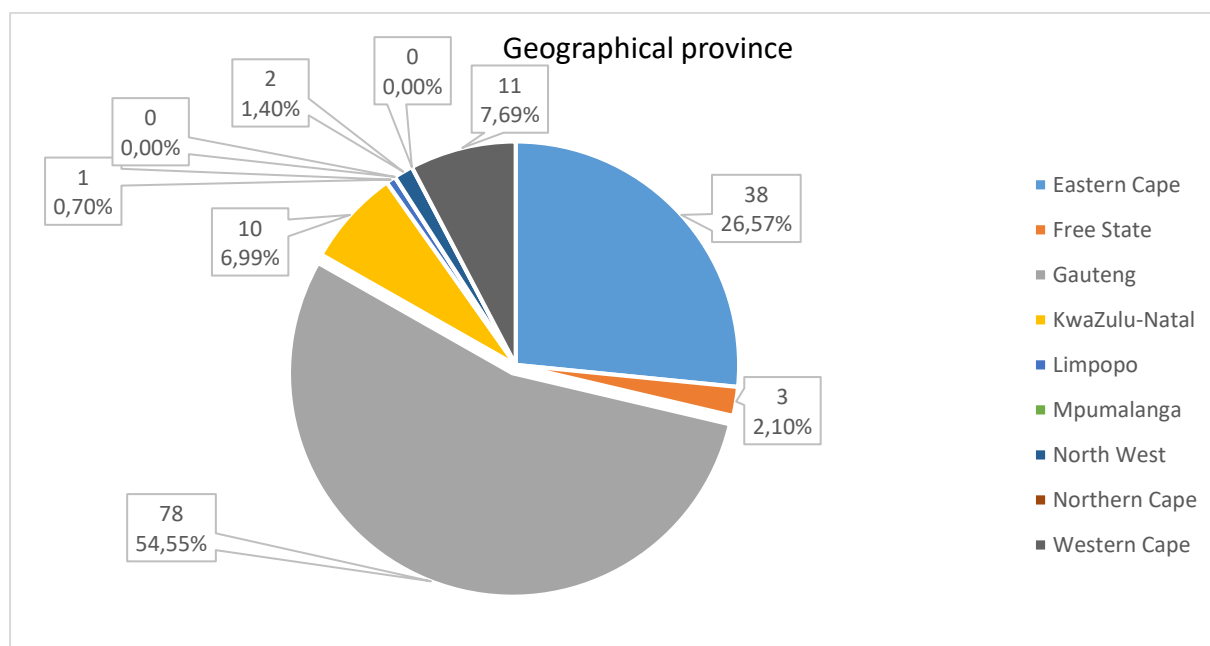


Figure 3.4: Geographical Province

Gauteng has the highest response number of respondents, with 78 respondents, followed by the Eastern Cape with 38 respondents. Two provinces (Mpumalanga and Northern Cape) had zero respondents.

3.3.3 Gender

Figure 3.5 indicates that, of the 143 respondents, 65 (45.45%) were male, compared with 78 (54.55%) females.

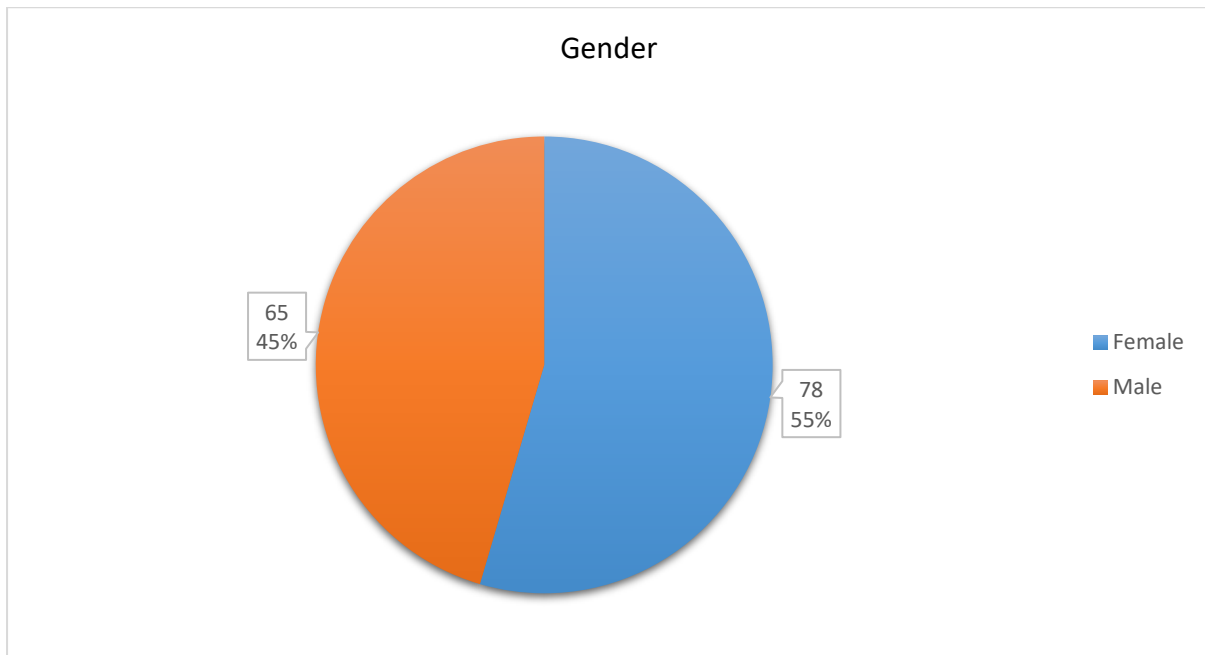


Figure 3.5: Gender

3.3.4 Currently or previously a member of medical aid

In Figure 3.6, it can be seen that of a total of 143 respondents, only 130 (90.91%) respondents are currently on medical aid and 13 (9.09%) respondents have previously been on medical aid.

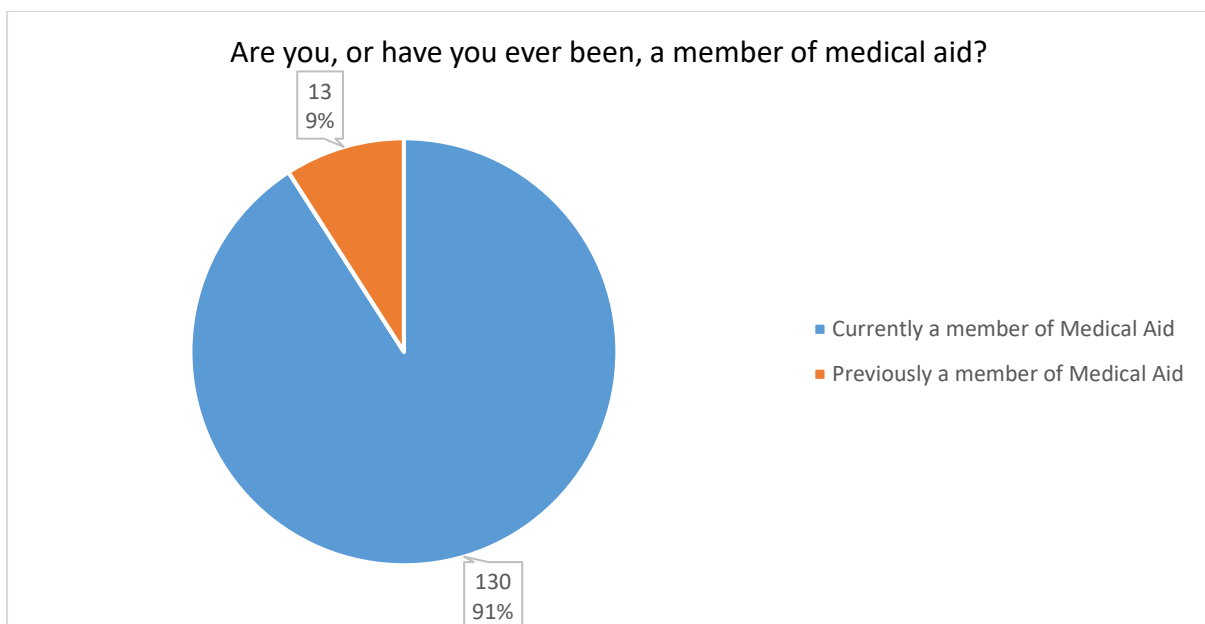


Figure 3.6: Membership of Medical aid

Chapter 3: Level of Awareness in the Private Healthcare Sector

Table 3.1 identifies a list of the top 10 medical aid to which respondents belong and the respondents' total count associated with these medical aid. The remaining medical aid are categorised and identified as 'Other' with a total membership of 25. The majority of the respondents belong to the Discovery medical aid.

Table 3.1: *List of Medical Aid Membership Counts*

Medical aid organization	Total
Discovery	67
Momentum	11
GEMS	8
BONITAS	7
Profmed	6
FedHealth	6
BestMed	6
Sizwe	3
Medshield	2
Bankmed	2
Other	25
Total	143

3.4 Results Part 2 – Background

This section indicates whether the respondents have heard about medical identity theft before and whether they understand the definition.

3.4.1 Have you previously heard the term “medical identity theft?”

For this question, the respondents have to indicate whether they have heard of medical identity theft.

Chapter 3: Level of Awareness in the Private Healthcare Sector

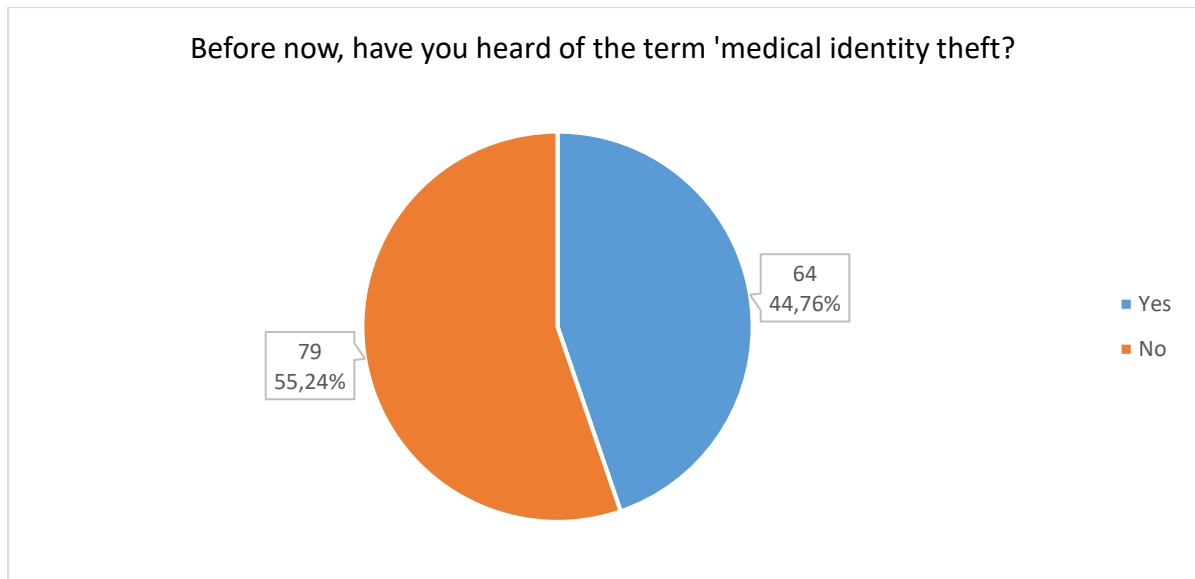


Figure 3.7: Previous Knowledge of Medical Identity Theft?

Figure 3.7 depicts a total of 143 respondents, of which 64 (44.76%) answered 'Yes' and 79 (55.24%) answered 'No' as to whether they had heard of medical identity theft before the survey.

Four respondents indicated the following in verbatim quotes made in response to the open-ended question at the end of the survey (as discussed further in section 3.7.24):

"I did not know this issue existed."

"I was unaware about medical identity theft but note that it could potentially increase due to the economy and waiting periods at public health providers."

"This was a bit of a surprise and opened my eyes to the possibility of the theft of our medical information"

"I did not even know that it exist."

These results indicate that more than half of the respondents were unaware that medical identity theft even existed.

3.4.2 Do you know the definition of medical identity theft?

This question determines whether the respondents had previously known the definition of medical identity theft.

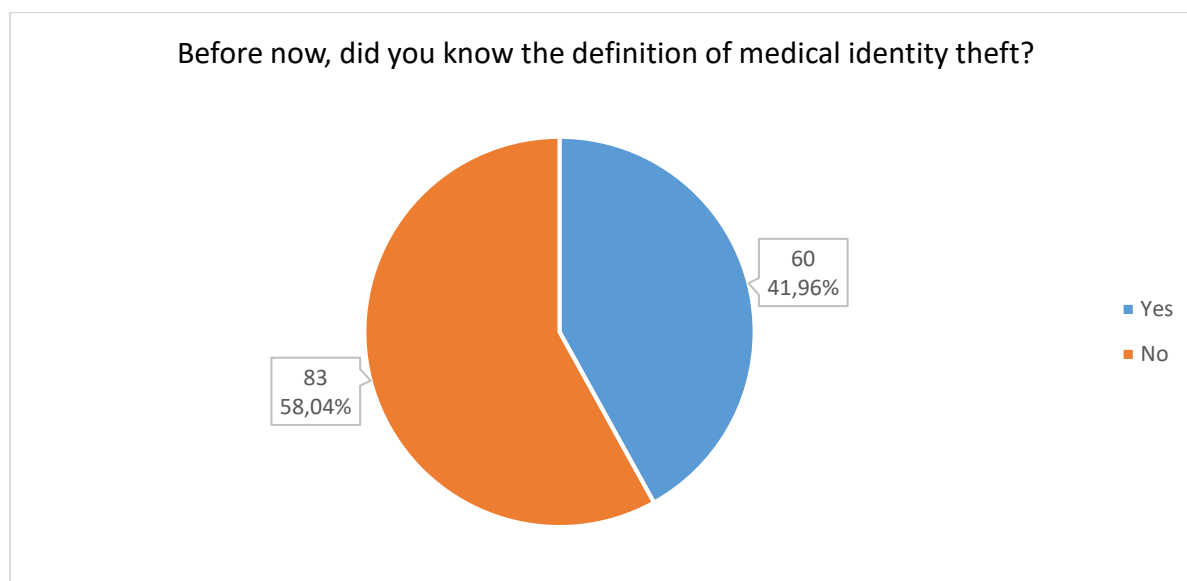


Figure 3.8: Level of Awareness of Medical Identity Theft

Figure 3.8 depicts a total of 143 respondents, of whom 60 (41.96%) answered positively, namely that they had known what medical identity theft was and 83 (58.04%) who indicated that before now, they had not known the definition of medical identity theft.

Therefore the definition of medical identity theft is not widely known in South Africa.

A total of 60 respondents who selected 'Yes', were transferred to section 3.4.3, once the respondents had completed the questions. The remaining 83 respondent who selected the 'No' option continued to 3.4.4, along with the other 60 respondents.

3.4.3 If 'Yes', how did you learn about medical identity theft?

The purpose of this question was to understand how the respondents learnt of medical identity theft, based on the previous question. The question allows a respondent to have multiple selections of the options.

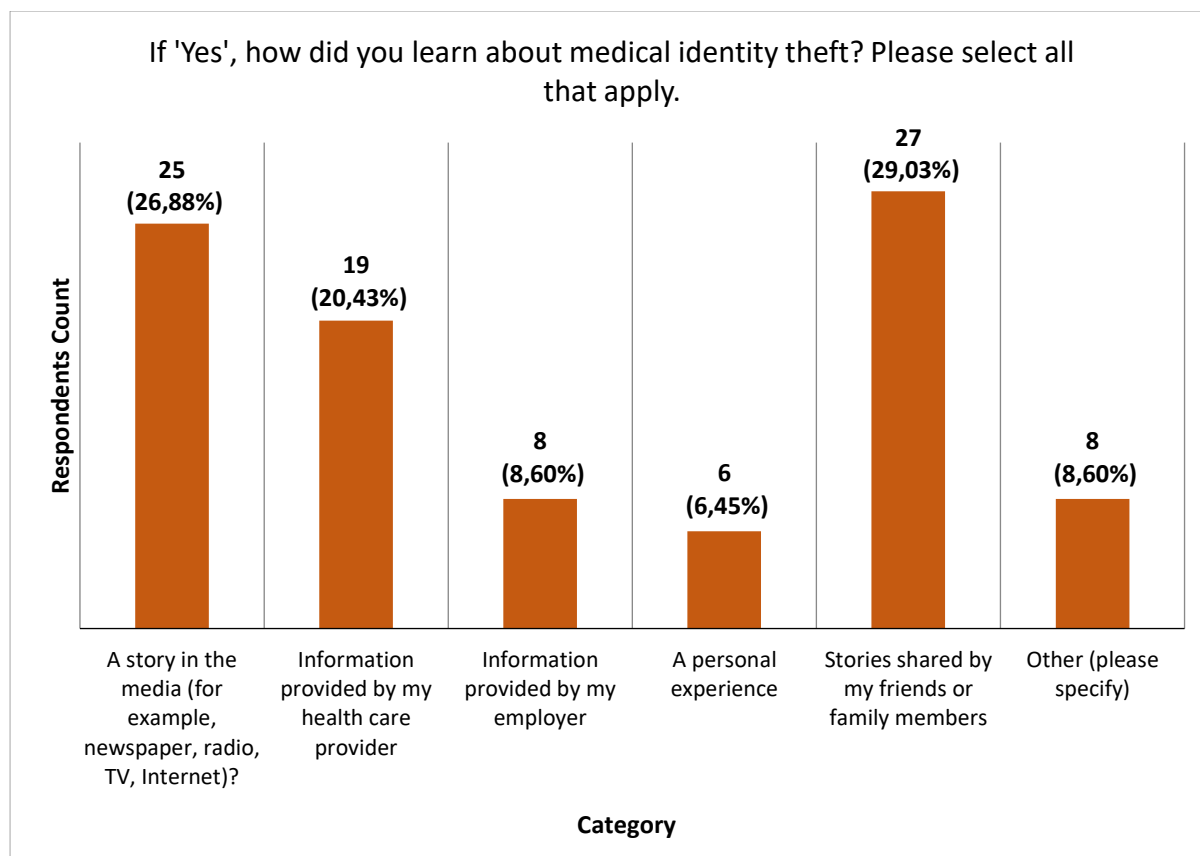


Figure 3.9: Sources of Information for Medical Identity Theft

Figure 3.9 identifies how the respondents learnt about medical identity theft. The results from 60 respondents are as follows:

- 25 (26.88%) respondents selected ‘a story in the media’.
- 19 (20.43%) respondents selected ‘information provided by health care provider’.
- 8 (8.6%) respondents selected ‘information provided by employer’.
- 6 (6.45%) respondents selected a ‘personal experience’.
- 27 (29.03%) respondents selected ‘stories shared by respondents’ friends or family members’.
- 8 (8.6%) respondents selected ‘Other’, as mentioned in section 3.2.1. Listed below are the following relevant verbatim quotes:

“Legal Profession”

“I am a data professional who has seen cases in my analysis”

“I work for an Identity Management Company”

“Working for medical practice”

“I am a medical practitioner. I have had patients attempting to commit this type of fraud”

The highest response rate is 29.03% of respondents who selected shared stories by friends and family. The second highest response rate is 26.88% for learning of medical identity theft by a story in the media. A respondent indicated “Legal Profession”, as the way he learnt of medical identity theft was through his law studies. The other respondents from the verbatim quotes indicate that the way they learnt of medical identity theft was through work experience, namely incidents of the occurrence of medical identity theft or through data analysis.

South Africans are generally not yet familiar with medical identity theft or have not personally experienced it.

3.4.4 Actions performed if aware your medical records were lost or stolen

The purpose of this question would be to identify the two most important actions to take if the respondents were informed of their medical records being lost or stolen. This question allowed respondents to choose two options.

Chapter 3: Level of Awareness in the Private Healthcare Sector

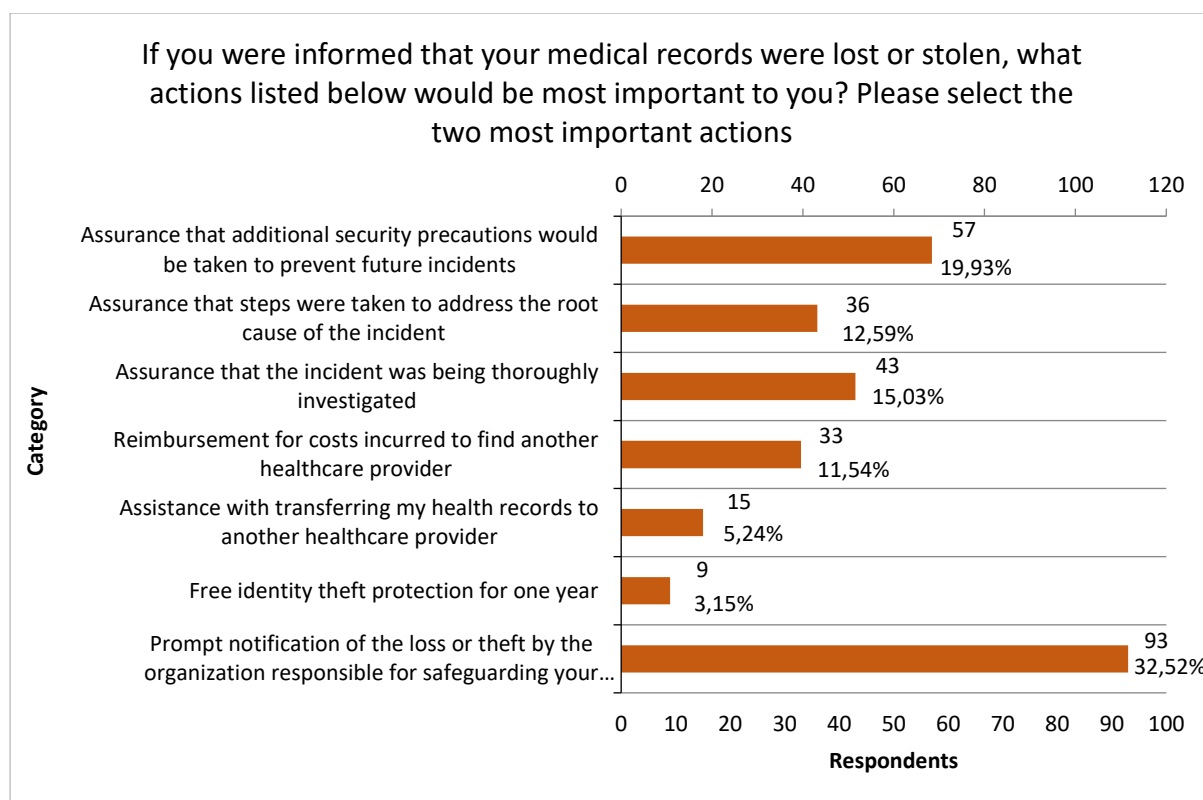


Figure 3.10: Appropriate Actions After Theft of Medical Records

Figure 3.10 describes which actions would be considered important by respondents on learning of the loss of their medical records. The results from 143 respondents as follows:

- 57 (19.93%) respondents selected ‘assurance that additional security precautions will be taken to prevent future incidents’.
- 36 (12.59%) respondents selected ‘assurance that steps were taken to address the root cause of the incident’.
- 43 (15.03%) respondents selected ‘assurance that the incident was being thoroughly investigated’.
- 33 (11.54%) respondents selected ‘reimbursement for cost incurred to find another healthcare provider’.
- 15 (5.24%) respondents selected ‘assistance with transferring their health records to another healthcare provider’.
- 9 (3.15%) respondents selected ‘free identity theft protection for one year’.
- 93 (32.52%) respondents selected ‘prompt notification of the loss or theft by the organization responsible for safeguarding your confidential information (within 30 days)’.

Chapter 3: Level of Awareness in the Private Healthcare Sector

Two respondents to the open-ended question (described further in section 3.7.24) indicated the following:

“If there is an incident of medical identity theft (of my records) and medical benefits are used, I would like to have insurance cover which pays for that expense so that I am not held accountable for the amount.”

“Medical Identity theft insurance should ideally be standard with all medical aid schemes.”

From the verbatim quotes it appears the respondents would prefer the medical aid to offer insurance for medical identity theft. Therefore using free identity theft protection can help inform respondents when an incident occurs. It will also offer the assurance that future possibilities of identity theft will be reduced.

The highest response rate of 32.52% was for prompt notification of the loss or theft by the organization responsible for safeguarding confidential information. This was followed by 19.93% who selected assurance that additional security precautions would be taken to prevent future incidents.

This indicates that the respondents want the organization to take responsibility for the issue and notify members immediately thereby allowing the victims to decide how to proceed further.

3.4.5 Inaccuracies caused by medical identity theft in your medical records

This question focuses on the respondents' awareness of the possibility that medical identity theft can compromise personal private medical records.

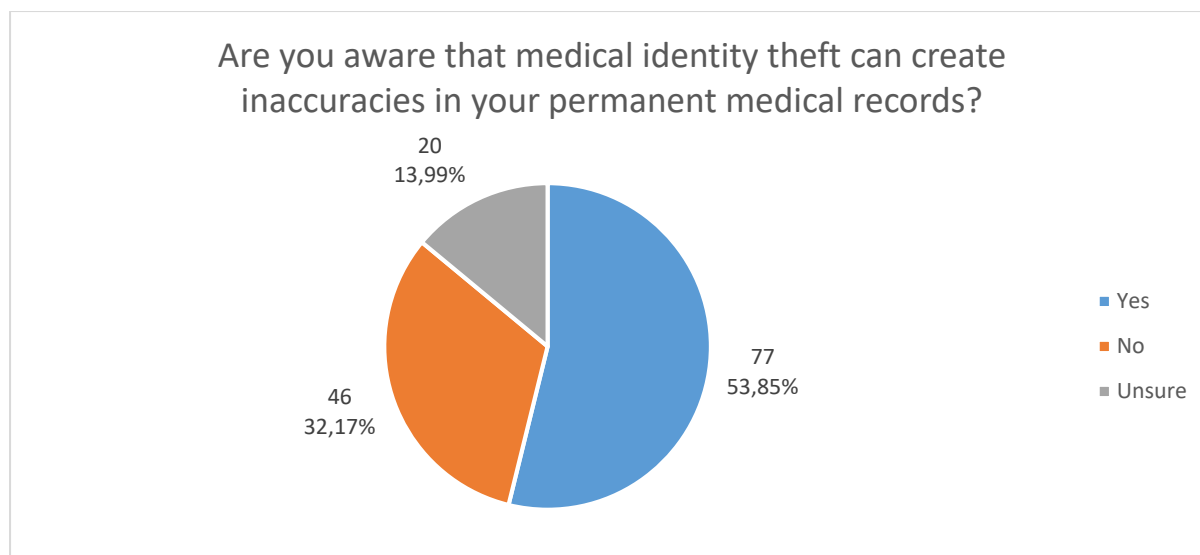


Figure 3.11: Awareness of Consequences of Medical Identity Theft

Figure 3 depicts the levels of awareness of inaccuracies in the medical records and their consequent devastating effects for the medical aid members, healthcare industry and health professionals. The results from 143 respondents are as follows:

- 77 (53.85%) respondents selected 'Yes'.
- 46 (32.17%) respondents selected 'No'.
- 20 (13.99%) respondents selected 'Unsure'.

Respondents show a 53.85% response rate of being aware that medical identity theft can create inaccuracies. A significant percentage of 46.15% respondents are unsure or unaware that inaccuracies can happen.

3.5 Results Part 3 – Healthcare Provider Privacy

This section seeks to determine the respondents' level of interaction with the healthcare provider such as hospitals or clinics and whether documents are checked regularly.

3.5.1 Checking your medical records are accurate

The purpose of this question is to gauge whether the respondents verify their medical records of personal health and whether the information has been correctly recorded by the healthcare provider.

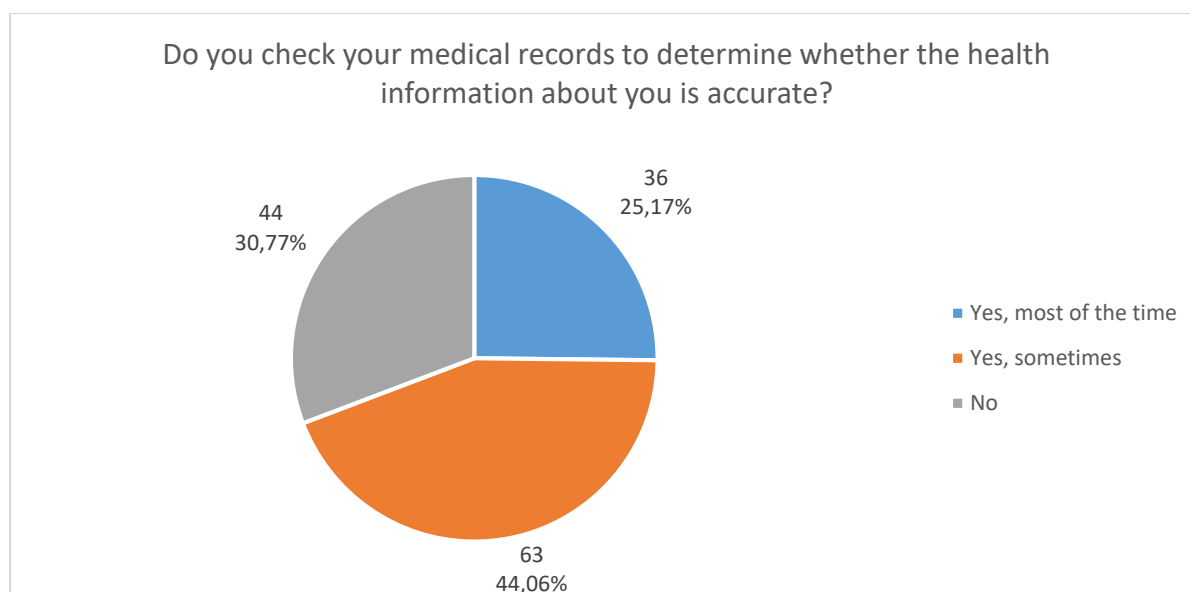


Figure 3.12: Accuracy of Personal Health Information

This section indicates how many respondents check their health information in their medical records. The regular checking of medical records will allow enable them to notice whether their personal health information contains any inaccuracies. The results from 143 respondents as depicted in Figure 3.12 are as follows:

- 36 (25.17%) respondents selected 'Yes, most of the time'.
- 63 (44.06%) respondents selected 'Yes, sometimes'.
- 44 (30.77%) respondents selected 'No'.

South African respondents generally check their medical health information regularly with 25.17% and 44.06% responding 'Yes'. Only about 30.77% of the respondents do not check their medical records.

A total of 44 respondents who selected 'No' were transferred to section 3.5.2, and the remaining 99 respondents who selected 'Yes', were transferred to section 3.5.3. Once all respondents had completed the required question, they were joined up again at section 3.5.4.

3.5.2 Why don't you check?

The purpose of this question is to gain an understanding as to why the respondents do not check their health information. This question only applied to the respondents who selected 'No' in the previous section. The question allows a respondent to have multiple selections of the options.

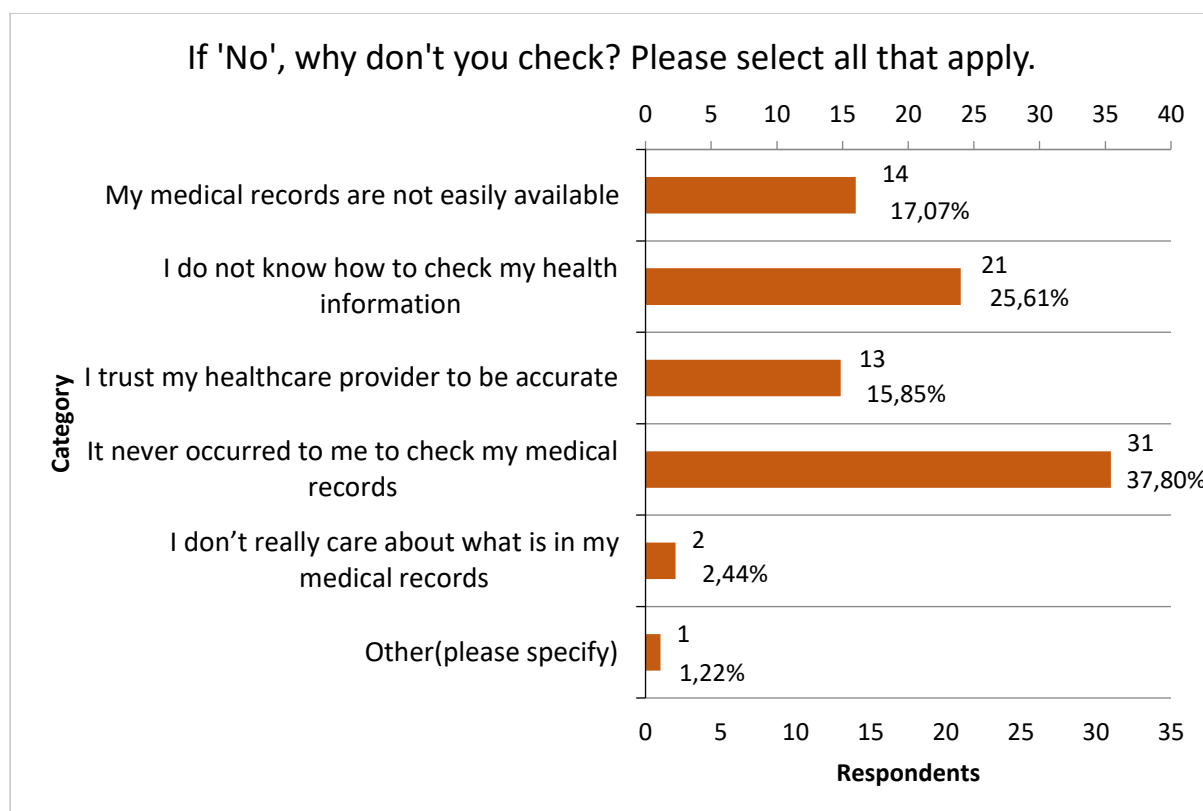


Figure 3.13: Reasons for Not Checking Own Medical Records

In Figure 3.13, the reason why respondents do not check their medical records were identified. The results from 44 respondents are as follows:

- 14 (17.07%) respondents selected 'My medical records are not easily available'.
- 21 (25.61%) respondents selected 'I do not know how to check my health information'.
- 13 (15.85%) respondents selected 'I trust my healthcare provider to be accurate'.
- 31 (37.80%) respondents selected 'It never occurred to me to check my medical records'.
- 2 (2.44%) respondents selected 'I don't care about what is in my medical records'.
- 1 (1.22%) respondent selected 'Other'.

The highest response rate was 37.80%, indicating that it never occurred to the respondents to actually check their medical records. The second highest selection at 25.61% reveals that the respondents did not know how to check their personal health information. The lowest response rate option was the respondents who did not care about the medical records, which amounted to 2.44% of the respondents in SA.

With the high response rate in SA for never checking one's medical records, this could indicate medical aid members never considered that checking their records is important. They trusted their healthcare provider with the accuracy of the information.

3.5.3 How do you check?

In understanding how respondents check their health information this question only applied to the respondents who selected 'Yes' from section 3.5.1. The question allowed respondents to have multiple selections of the options.

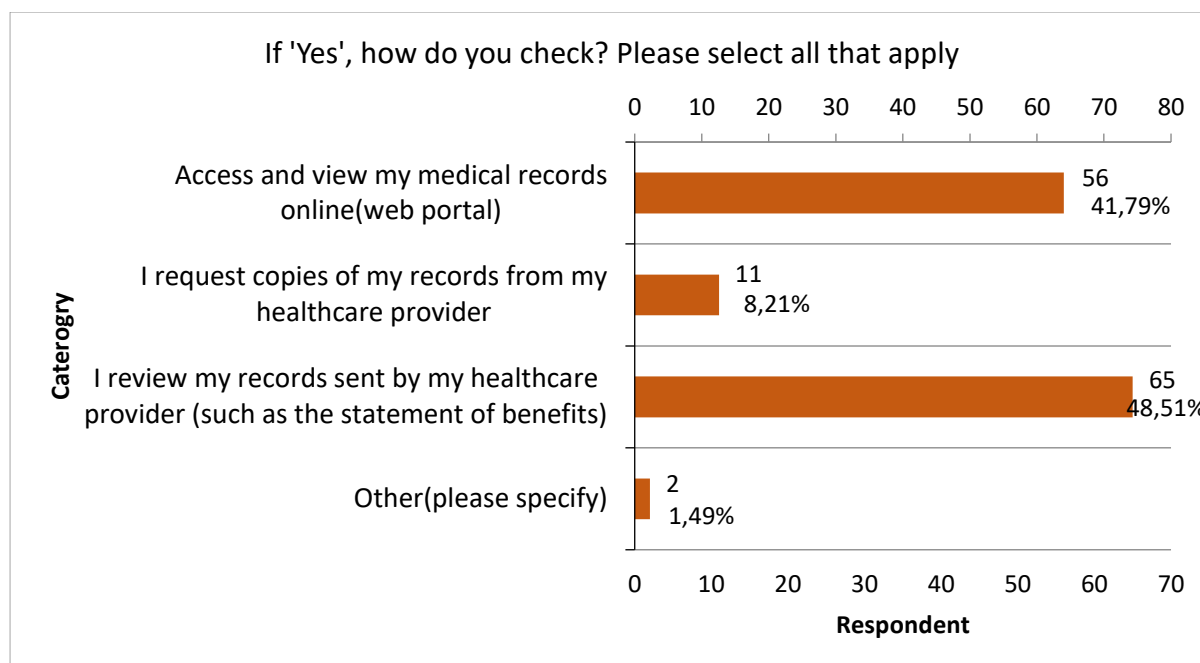


Figure 3.14: How Medical Records Are Checked

Figure 3.14 identifies how respondents check their medical records. The results from 99 respondents are as follows:

- 56 (41.79%) respondents selected access and view medical records online (web portal).
- 11 (8.21%) respondents selected I request copies of records from healthcare provider.
- 65 (48.51%) respondents selected I review records sent by healthcare provider (such as the statement of benefits).
- 2 (1.49%) respondents selected other.

Chapter 3: Level of Awareness in the Private Healthcare Sector

The highest response rate was 48.51% of respondents who review the records sent by the healthcare provider (example, SOB). The second highest group (41.79%) access and view their medical records online (example, web portal).

The response shows that allowing medical aid members access to a healthcare portal facilitates members checking their healthcare records from the healthcare provider frequently.

3.5.4 Rate the statement of healthcare provider

This section focuses on three questions using a Likert scale to obtain respondents' expressions of 'strongly disagree' to 'strongly agree' based on the question. The results are displayed on a stacked chart, which reflects 143 respondents who participated.

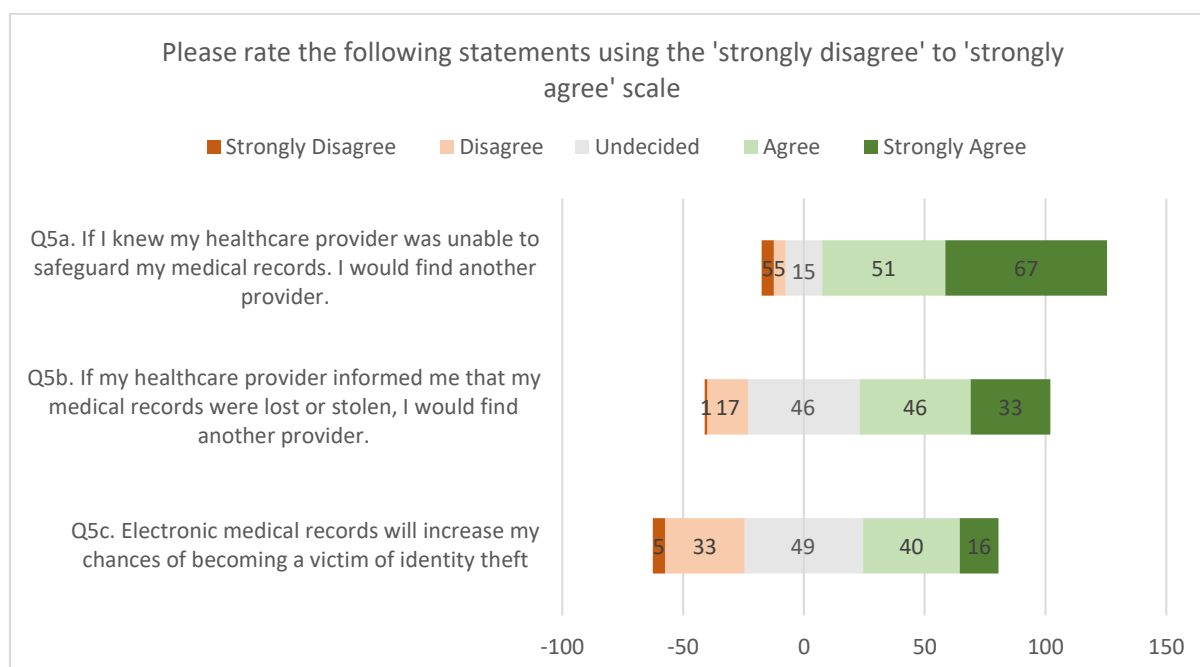


Figure 3.15: Respondents' Level of Trust of Healthcare Provider Scale

Regarding question 5a, a high response rate of 67 respondents choose 'strongly agreed' that if a healthcare was unable to safeguard personal medical records, respondents would find another provider. The next question, 5b, shows an equal rate of 46 respondents between 'undecided' and 'agree' namely if the healthcare provider informed the respondents that the medical records were lost or stolen, the respondents would find another provider. For the last question, 5c, the highest response rate of 49 respondents choose 'undecided' as to whether electronic medical records would increase their chances of becoming a victim of identity theft.

Chapter 3: Level of Awareness in the Private Healthcare Sector

This could possibly indicate that respondents need their medical aid and healthcare providers to guarantee that their data is constantly protected, Should anything unforeseen happen and the medical aid cannot protect the members, they would rather change to another medical aid provider who can ensure the safety of their information.

3.5.5 Importance of the following issues

This section focuses on two questions using a Likert scale to obtain respondents' ratings of 'irrelevant' to 'very important', based on the question. The results of the 143 respondents are displayed on a stacked chart.

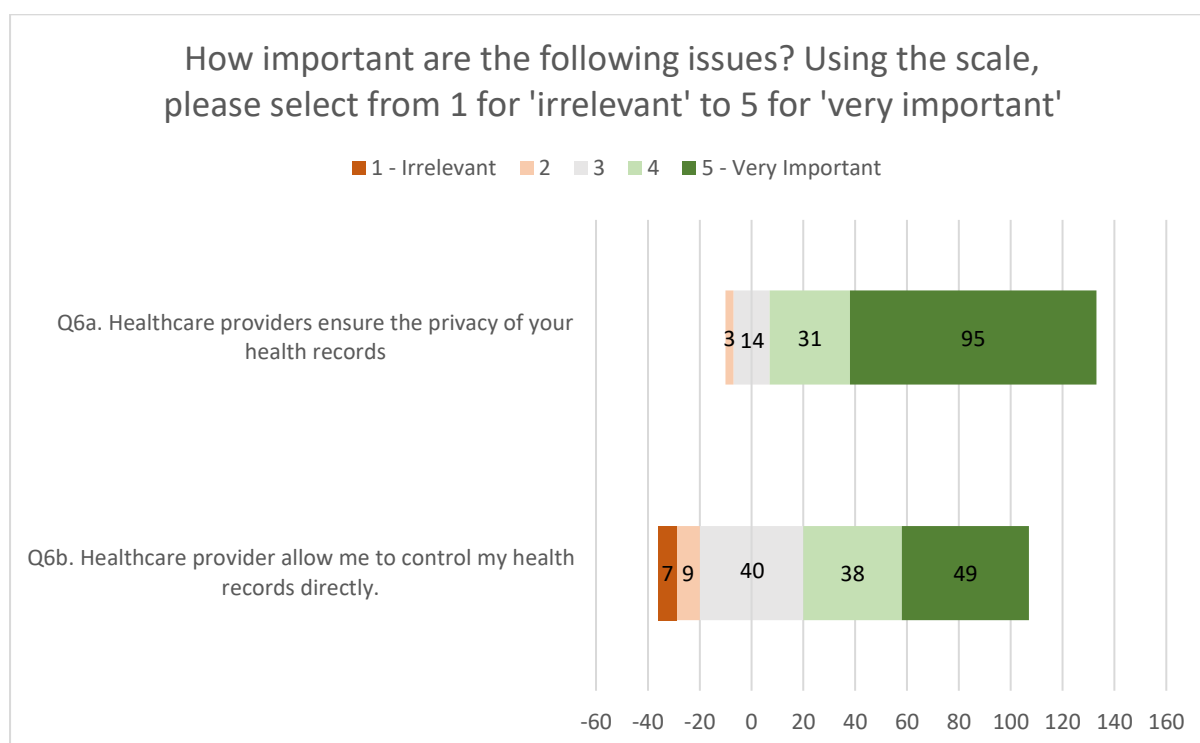


Figure 3.16: Respondents' Ratings Importance Relating to Health Records Scale

Regarding question 6a, a high response rate of 95 respondents chose 'very important' for a healthcare provider to ensure the privacy of the respondents' health records. For the next question, 6b, 49 of the respondents would be in favour of the healthcare provider allowing the respondents to control their health records directly.

Overall this could show that there are more respondents who trust their health care providers to ensure the privacy of their health records while fewer would prefer to have direct control of their own records.

3.6 Results Part 4 – Medical Aid Privacy

This section measures the respondents' awareness of the contents of their SOB and their understanding of the full function of the benefits offered by the medical aid. It also identifies the type of coverage from their medical aid. Furthermore, it determines whether the respondents review their SOB when receiving their forms and whether they check all the critical information in the SOB.

3.6.1 Medical aid concern for medical identity theft

The purpose of this question, is to determine whether respondents are aware of their medical aid's concern in regard to medical identity theft incidents.

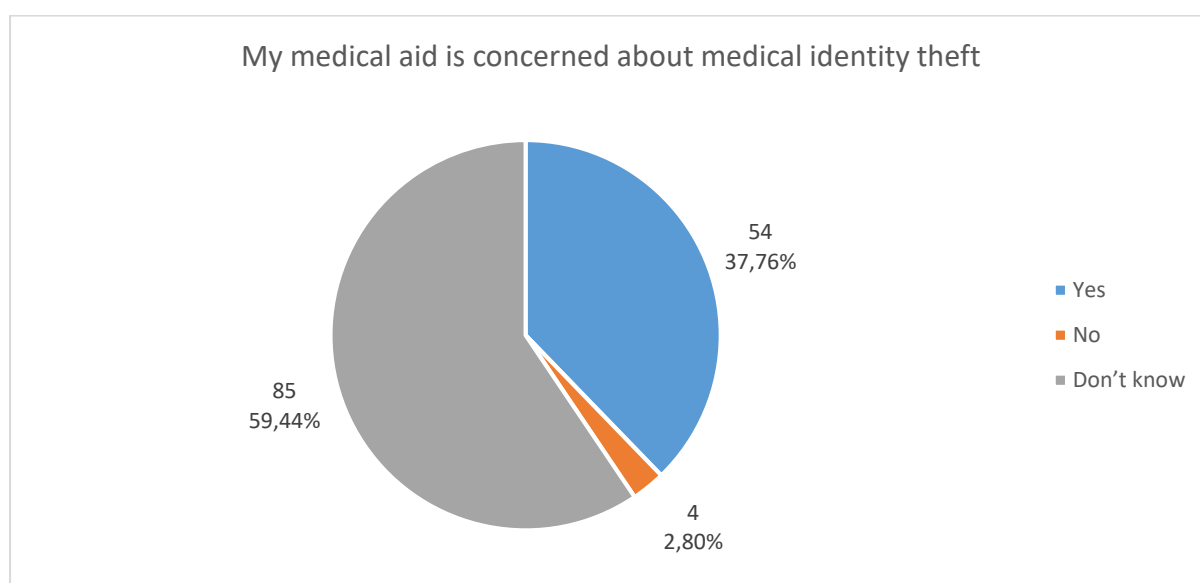


Figure 3.17: Medical Aid is Concerned About Medical Identity Theft

Figure 3.17 is based on the respondents' awareness of their medical aid's concern relating to medical identity theft. In addition, it determines whether the respondents have been informed about medical aid theft. The results from 143 respondents are as follows:

- 54 (37.76%) respondents selected 'Yes'.
- 4 (2.80%) respondents selected 'No'.
- 85 (59.44%) respondents selected 'Don't know'.

Only 37.76% of the respondents indicated that their medical aid are concerned about medical identity theft, whereas 2.80% of respondents indicated their medical aid is not concerned. The majority of respondents (59.44%) indicated that they are unaware if their medical aid is concerned about medical identity theft. This could be that the

majority of medical aid do not inform medical aid members of crimes such as medical identity theft.

Therefore, four (4) respondents who selected the 'No' option were transferred to section 3.6.2, to re-join the remaining 139 respondents at 3.6.3.

3.6.2 If 'No', would you consider changing

Based on the previous selection by respondents, if the respondents indicated that the medical aid is not concerned about medical identity theft, then the question determines whether the respondent would be willing to change their medical aid.

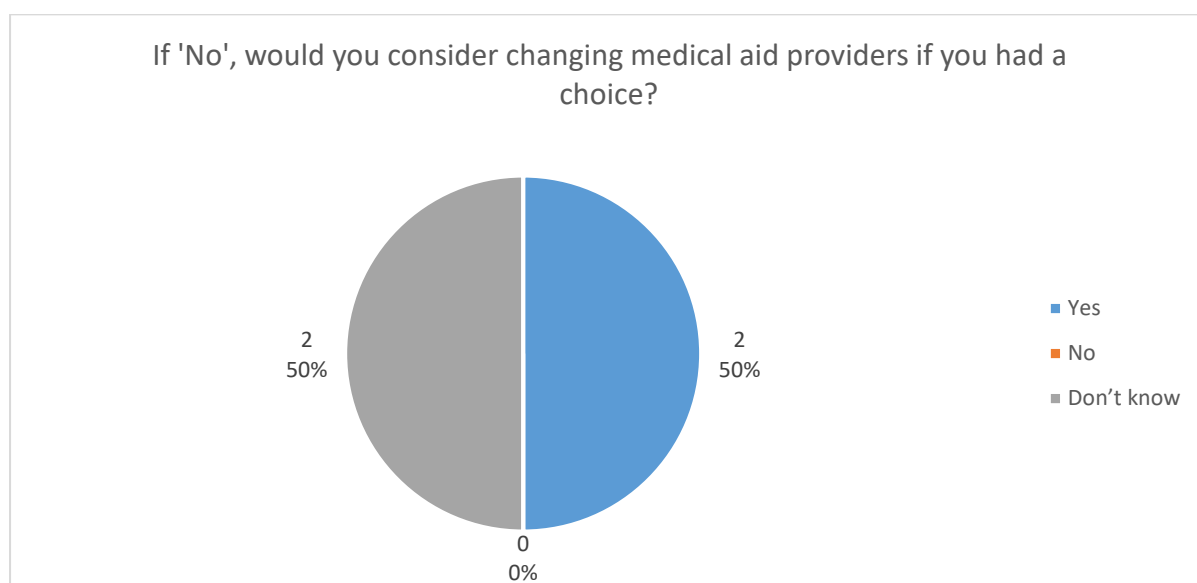


Figure 3.18 Changing Medical Aid Membership

Figure 3.18, based on the four respondents from the previous question, 50% of the respondents indicated that they would change to another medical aid and the remaining 50% respondents were uncertain as to whether they would change their medical aid. The results are as follows:

- 2 (50%) respondents selected 'Yes'.
- 0 (0%) respondent selected 'No'.
- 2 (50%) respondents selected 'Don't know'.

A respondent from section 3.7.24 indicated the following:

"I would be unable to change my medical aid provider as my condition would not be accepted by any other providers"

The respondent believed if he or she was a victim of medical identity theft, he or she could not change to another medical aid owing to a serious medical condition.

Zero per cent of respondents indicated that they would not change to another medical aid. Two (50%) respondents will change their medical aid and the other two (50%) respondents is uncertain whether they will change their medical aid if they had a choice.

3.6.3 Do you read your Statement of Benefit (SOB)?

This question gauges the respondents' level of awareness of the contents of their SOBs.

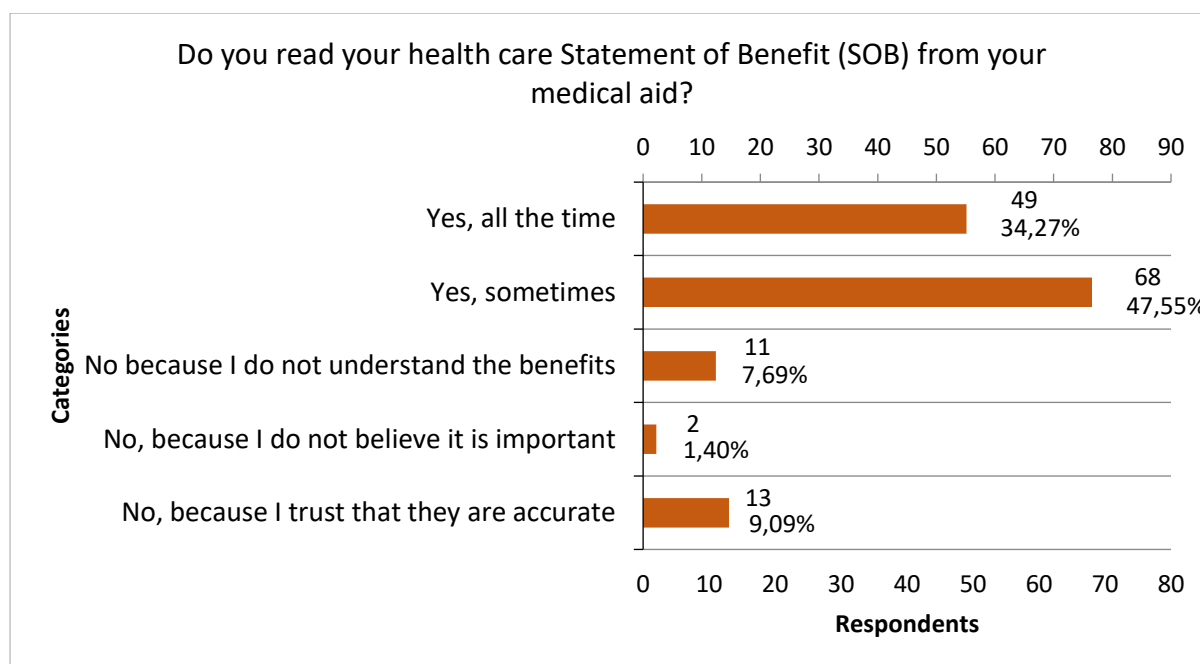


Figure 3.19: Level of Awareness of Contents of SOB

Figure 3.19, a total of 143 respondents provided feedback regarding their SOBs from the medical aid. The results are as follows:

- 49 (34.27%) respondents selected 'Yes, all the time'.
- 68 (47.55%) respondents selected 'Yes, sometimes'.
- 11 (7.69%) respondents selected 'No', as the respondents did not understand their SOBs.
- 2 (1.4%) respondents selected 'No', as the respondents believe it is not important to check.
- 13 (9.09%) respondents selected 'No', as the respondents trust that the medical records are accurate.

Chapter 3: Level of Awareness in the Private Healthcare Sector

A very high percentage (81.82%) or 117 respondents check their SOB, whether all the time (34.27%) or sometimes (47.55%). A very low percentage (18.18%) or 26 respondents do not check their SOB or do not really care about the accuracy.

Not checking one's SOB when receiving it can possibly lead to medical identity theft not being spotted. Identifying mistakes in one's record timeously can possible lead to a speedy solution.

A total of 117 respondents who selected the 'Yes' option (both 'Yes, all the time' and 'Yes, sometimes'), were transferred to section 3.6.4 and re-joined the remaining respondents at 3.6.5. The remaining 26 respondents who selected the 'No' option (either, 'No because I do not understand the benefits', 'No, because I do not believe it is important' or 'No, because I trust they are accurate') continued to 3.6.5, along with the other 117 respondents.

3.6.4 If 'Yes', which one is the most important to ensure the SOB is correct?

Based on the previous selection from respondents, if the respondent selected 'Yes, all the time' or 'Yes, sometimes' regarding checking the SOB from medical aid, then the question here would identify what information the respondent regards as the most important to ensure the SOB is correct.

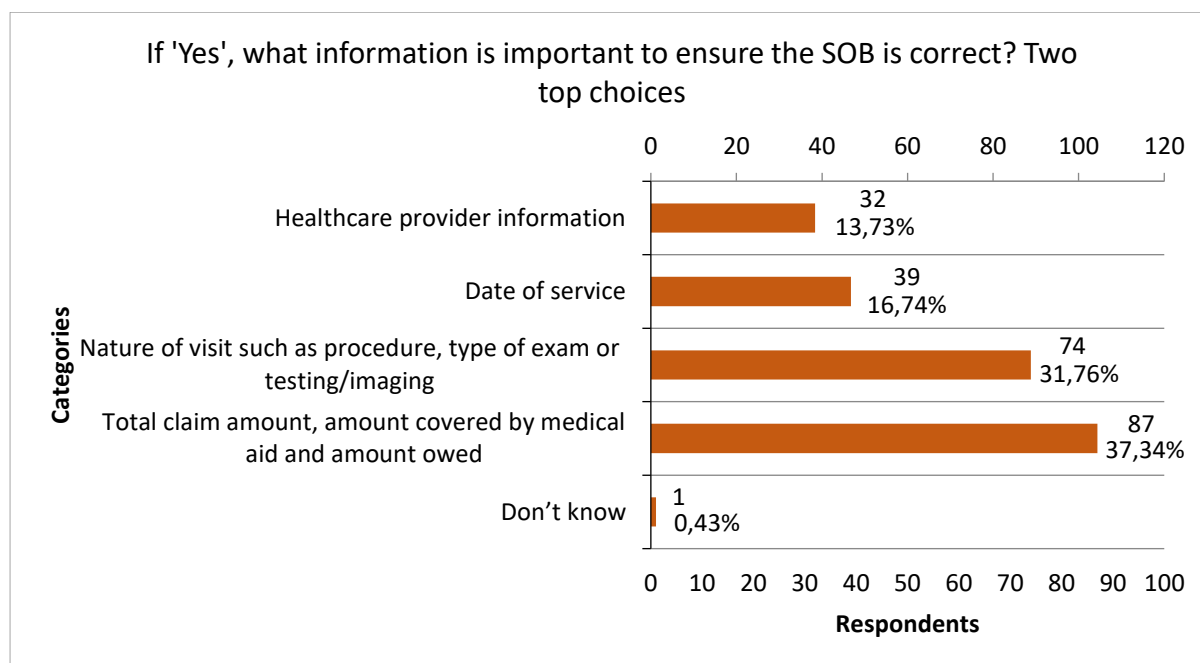


Figure 3.20: Importance of Correct SOB Information

Figure 3.20 is based on the 117 respondents from the previous question. These respondents selected two options each or else 'Don't know' which counted as one

option. The choices that respondents considered to be the most important for an SOB are as follows:

- 32 (13.73%) respondents selected 'Healthcare provider information'.
- 39 (16.74%) respondents selected 'Date of service'.
- 74 (31.76%) respondents selected 'Nature of visit such as procedure, type of exam or testing/imaging'.
- 87 (37.34%) respondents selected 'Total claim amount, amount covered by medical aid and amount owed'.
- 1 (0.43%) respondent selected 'Don't know'.

The top choice, with 87 respondents (37.34%), was ensuring the selected total amount claimed by healthcare, the coverage from medical aid and the amount owed by the medical aid patient were accurate. The second most popular choice, with 74 respondents (31.76%) was that the nature of the visit was accurate.

This could therefore indicate that respondents were more concerned about the financial implications than the actual details of the visit.

3.6.5 Review your SOB and see a claim not recognize from your healthcare provider

The question examines whether the respondents review claims on their SOB from their healthcare provider.

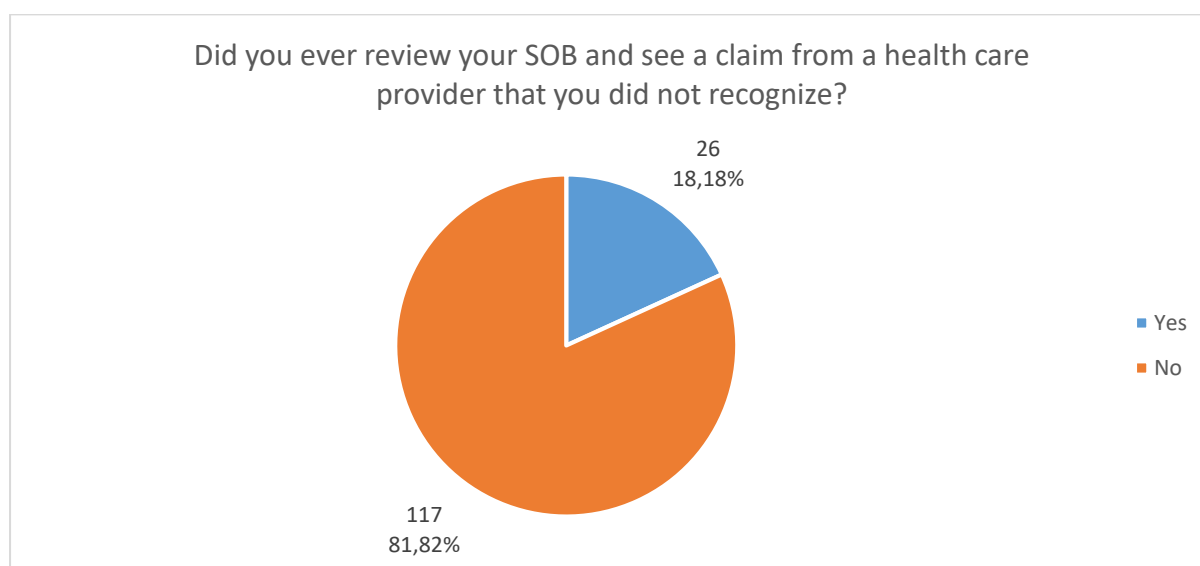


Figure 3.21: Reviewing Claims on SOB

Figure 3.21 consist of 143 respondents. It indicates whether respondents, when reviewing their SOB, have ever noticed a claim which they did not recognize. The results are as follows:

- 26 (18.18%) respondents selected 'Yes'.
- 117 (81.82%) respondents selected 'No'.

The majority of the respondents (81.82%) had no incidents of any claims which they did not recognize, while a very low response rate of 18.18% actually noticed an unfamiliar claim on their SOB.

Medical identity theft does not yet appear to be a problem in South Africa, although it is possible in the future that it can become a threat to SA medical aid members.

A total of 26 respondents who selected 'Yes' were transferred to section 3.6.6 and re-joined the remaining 117 respondents at 3.6.7. These remaining 117 respondents who selected the 'No' option continued to 3.6.7, along with the other 26 respondents.

3.6.6 If 'Yes', to whom did you report the claim?

The question determined to whom the respondents report the issues regarding unfamiliar claims on their SOB.

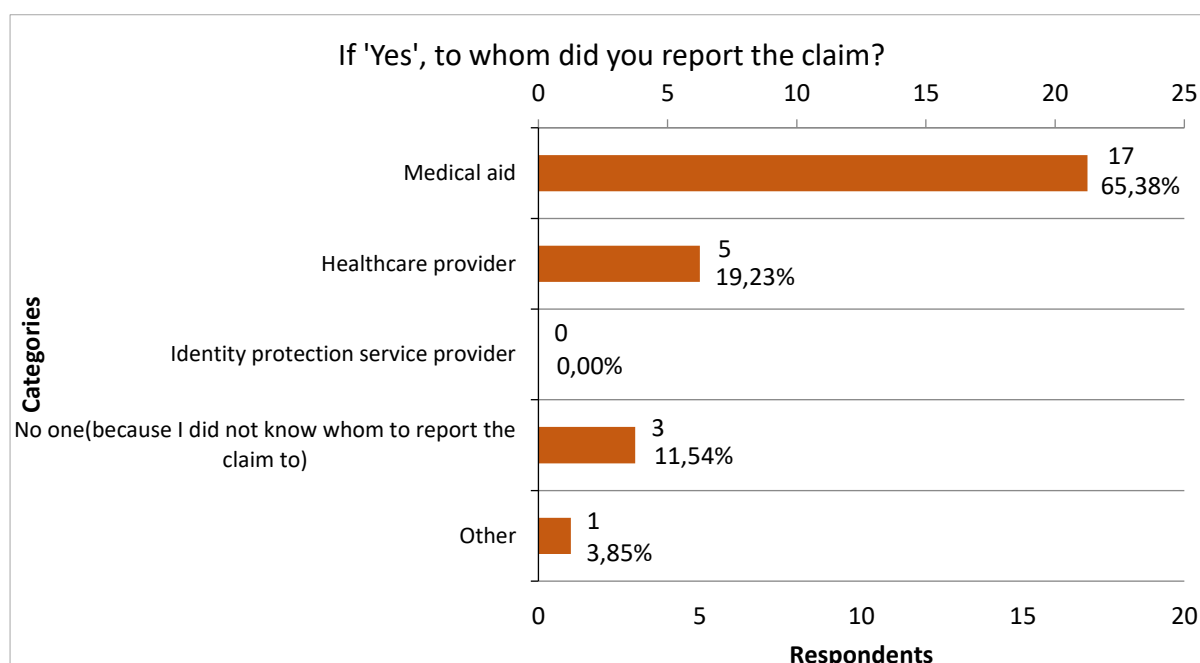


Figure 3.22: Reporting Unfamiliar Claims on SOB

Figure 3.22 refers to 26 respondents. Their responses are categorised as follows:

- 17 (65.38%) respondents selected 'Medical aid'.

Chapter 3: Level of Awareness in the Private Healthcare Sector

- 5 (19.23%) respondents selected 'Healthcare provider'.
- 0 (0.00%) respondent selected 'Identity protection service provider'.
- 3 (11.54%) respondents selected 'No one', as they were unsure who to report the claim to.
- 1 (3.85%) respondent selected 'Other'.

A very high percentage (65.38%) of respondents stated that they would report the claim to medical aid. They were followed by those (19.23%) preferring to report the matter to the healthcare provider.

The results could possibly indicate that reporting these issues directly to the medical aid or healthcare provider shows respondents' concern. They know that the cause of medical identity theft can lead to inaccuracies in their records as well as having financial implications.

3.6.7 Would you use a free medical identity theft monitoring service?

This question determines whether, if their medical aid had to offer a medical identity theft monitoring service for free, the respondents would be interested in using the service.

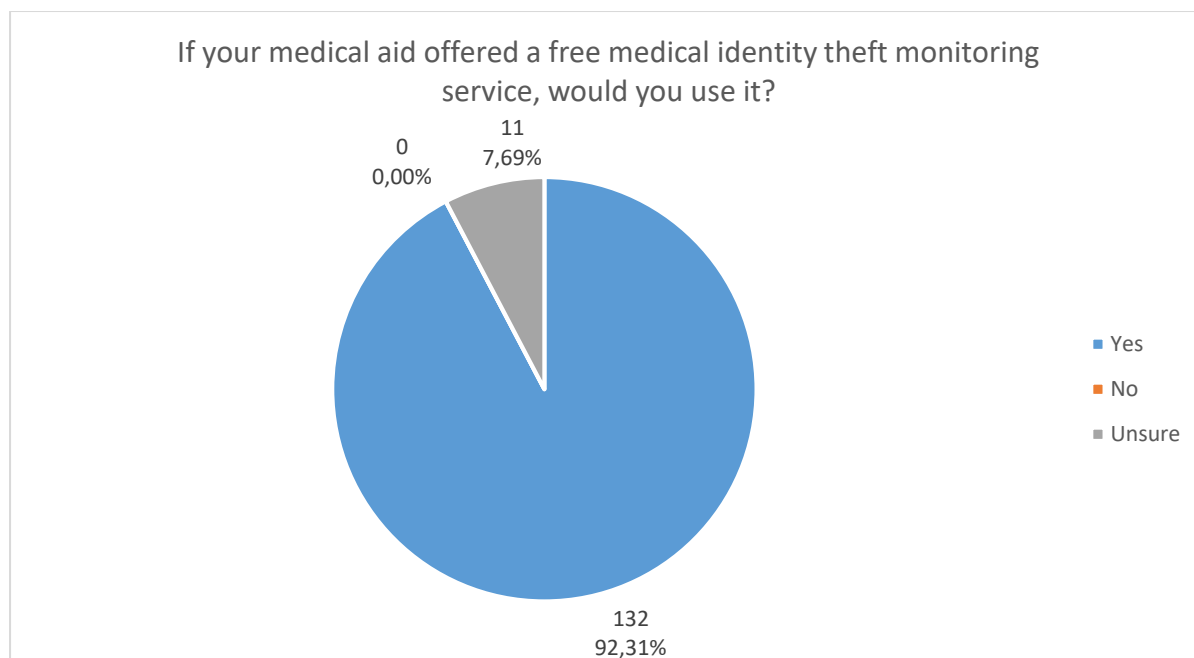


Figure 3.23: Support for Free Monitoring Service

Figure 3.23 refers to 143 respondents. It seeks to determine their possible support of a free medical identity theft monitoring service. The results are as follows:

- 132 (92.31%) respondents selected 'Yes'.
- 0 (0.00%) respondent selected 'No'.
- 11 (7.69%) respondents selected 'Unsure'.

With an extremely high response rate of 92.31% in favour, it is clear that an offer of a free medical identity theft monitoring service in SA would certainly be welcome. However, the remaining 7.69% of respondents were still unsure whether or not to use this service. It will take time for them to understand the functionality and how this can benefit them. There were no respondents who rejected the suggestion outright.

3.7 Results Part 5 – Medical Identity Theft Experience

This section focuses on the experiences of the respondents, whether personal or family related, and how much their total damages were as a result of medical identity theft.

3.7.1 Did you allow a family member to use your personal identity?

This question identifies whether the respondents knowingly allowed a family member to use their identity for medical services or medication assistance.

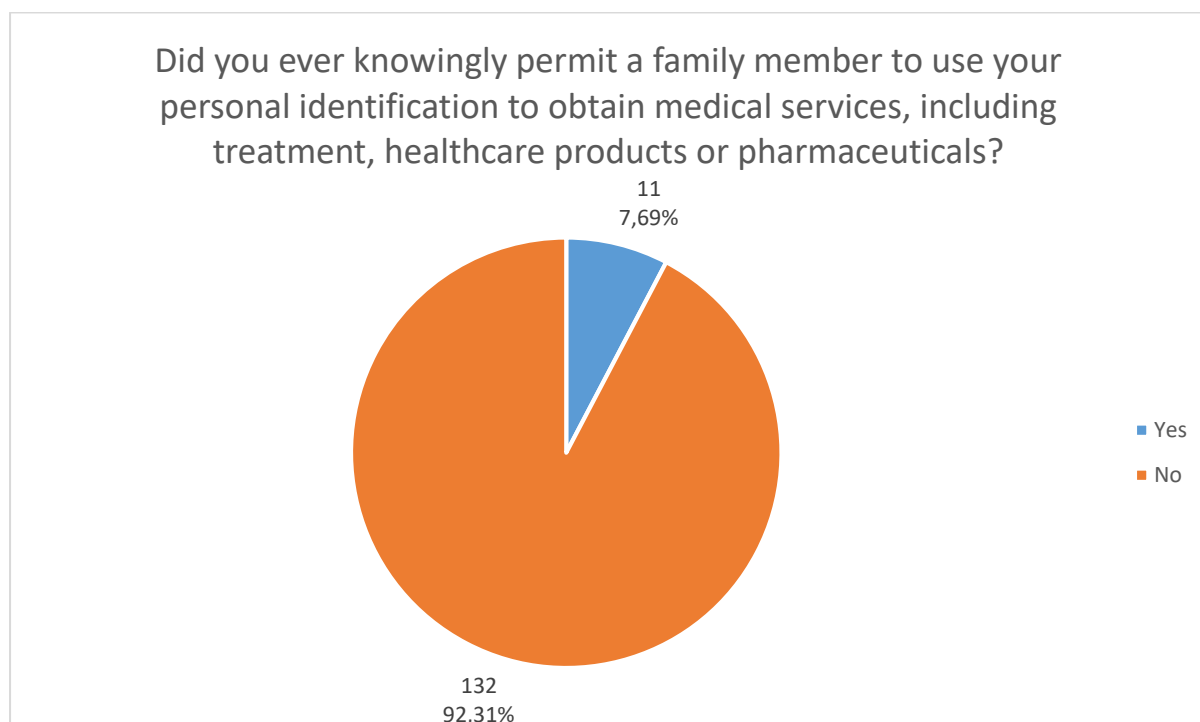


Figure 3.24: Use of Personal Identification by Family Members

Figure 3.24 refers to 143 respondents. The question identifies the use of members' personal information by family members for medical care treatment or medication. The results are as follows:

- 11 (7.69%) respondents selected 'Yes'.
- 132 (92.31%) respondents selected 'No'.

A very high response rate of 92.31% of respondents rejected the notion of allowing family members to use their personal information, while the remaining 7.69% admitted to letting family members use their identity for medical care.

This could be that the respondents want to help their family members without medical aid to ensure they get the care and treatment needed as confirmed in section 3.7.2.

A total of 11 respondents who selected 'Yes' were transferred to sections 3.7.2 and 3.7.3'. They were later re-joined by the remaining 132 respondents at section 3.7.4.

3.7.2 If 'Yes', why did you do this?

Based on the previous selection from respondents, if the respondent selected 'Yes for permitting family members to use their personal identity, then this question identified the reason for this. This question allows respondents multiple selections.

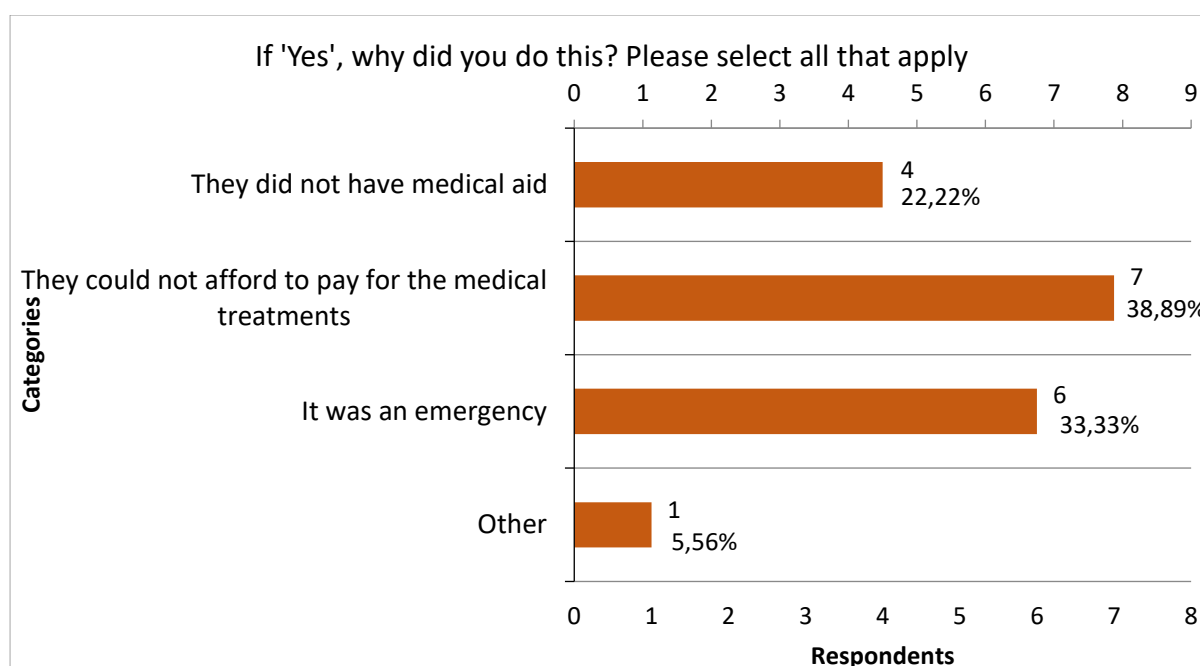


Figure 3.25: Reasons for Allowing Family Members to Use One's Personal Identity

Figure 3.25 refers to 11 respondents. The reasons for permitting family to use their personal identity are categorised as follows:

- 4 (22.22%) responded that they did not have medical aid.
- 7 (38.89%) responded that they could not afford to pay for the medical treatments.
- 6 (33.33%) responded that it was an emergency.

Chapter 3: Level of Awareness in the Private Healthcare Sector

- 1 (5.56%) respondent selected 'Other', as mentioned in section 3.2.1. A possible reason follows:

“Pharmaceutical purchases”

The highest response was 38.89% as the respondents felt the family member could not afford medical treatment so by allowing family members to use their personal identification for medical care, they were helping them. The next highest selection was 33.33% who explained that it was an emergency, so they allowed the family to use their medical aid. A respondent quoted “pharmaceutical purchases”, indicating he allowed a family member to use his medical aid for medication under his identity, as the family member possibly could not afford the medication, therefore he assisted by lending his medical aid.

Respondents could have possibly felt the need to help their family without medical aid as they needed the medical care assistance, either with medical service or pharmaceutical care.

3.7.3 If 'Yes', how often did you share your personal healthcare information with a family member

This question pertains to the 11 respondents from the previous question, which identifies how often the respondents allow their personal healthcare information to be shared with family.

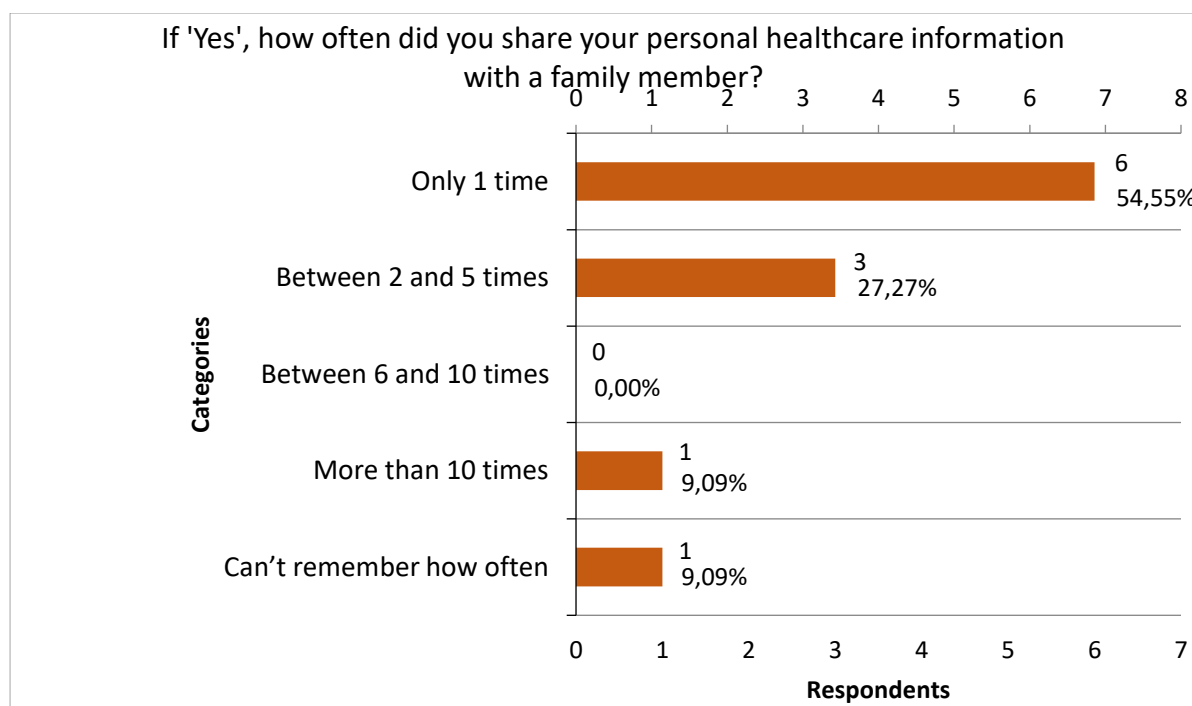


Figure 3.26: Frequency of Sharing Personal Healthcare Information

Figure 3.26 relates to 11 respondents, determining how often personal medical information is shared with a family member. The results are as follows:

- 6 (54.55%) respondents selected only 1 time.
- 3 (27.27%) respondents selected between 2 and 5 times.
- 0 (0.00%) respondent selected between 6 and 10 times.
- 1 (9.09%) respondent selected more than 10 times.
- 1 (9.09%) respondent selected can't remember how often.

The highest response rate of 54.55% indicated that the majority of the respondents only allowed a family member to use their personal medical information for medical care once. There were a few respondents who permitted the use of their personal medical information more frequently, ranging from between twice to more than 10 times

3.7.4 Did you allow a non-family member to use your personal identity

This question determines whether respondents allow other individuals who are not their family member to use their personal identity for medical care or medication.

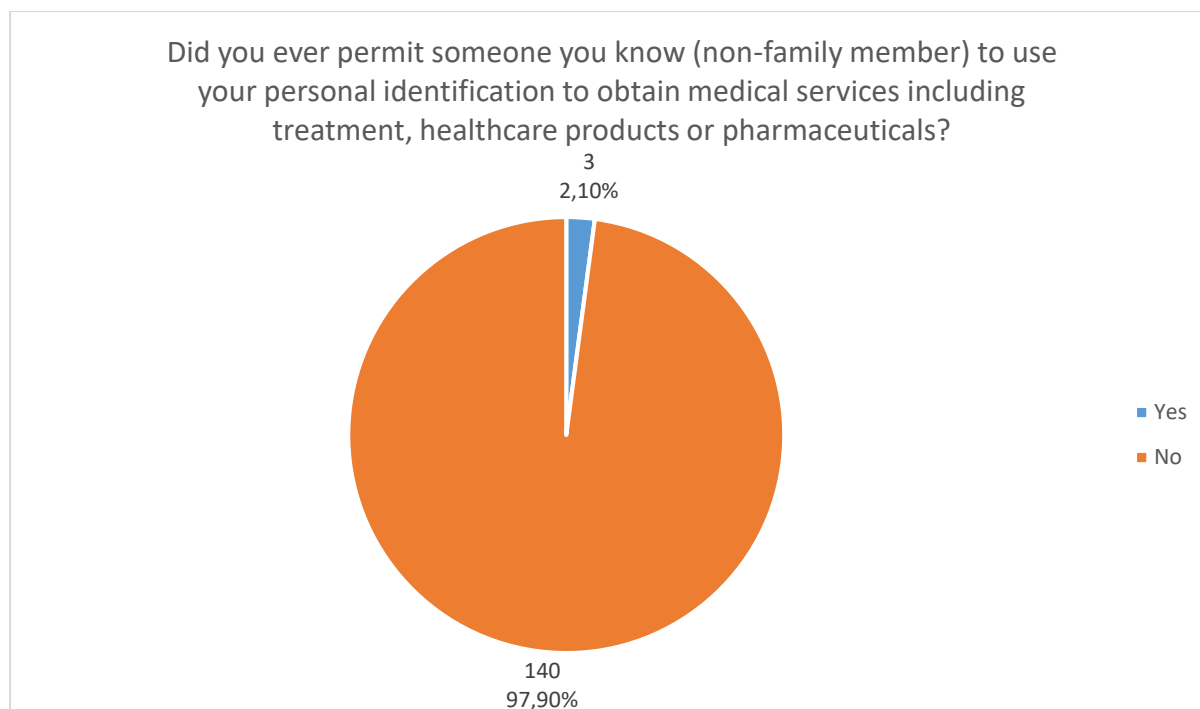


Figure 3.27: Use of Personal Medical Identity by Non-Family Members

Figure 3.27 refers to 143 respondents. It determines whether respondents shared their personal identity with someone they know who is not a relative. The results are as follows:

- 3 (2.10%) respondents selected 'Yes'.
- 140 (97.90%) respondents selected 'No'.

An extremely high proportion of respondents (97.90%) selected 'No', indicating that these respondents do not share personal information and medical benefits with other people who are not their family. Only 2.10% of the respondents indicated that they permitted someone not a family member to use their personal identity for medical care.

A total of 3 respondents which selected 'Yes', will be transferred to sections 3.7.5 and 3.7.6, once the respondents has completed these two questions, the remainder 140 respondents which selected 'No' option, will continue on section 3.7.7, along with the other 11 respondents.

3.7.5 If 'Yes', why did you do this?

Based on the previous section, if the respondent selected 'Yes', permitting non-family members to use their personal information, then the question here will identify the reason behind the respondents' decision. This question allows respondents multiple selections.

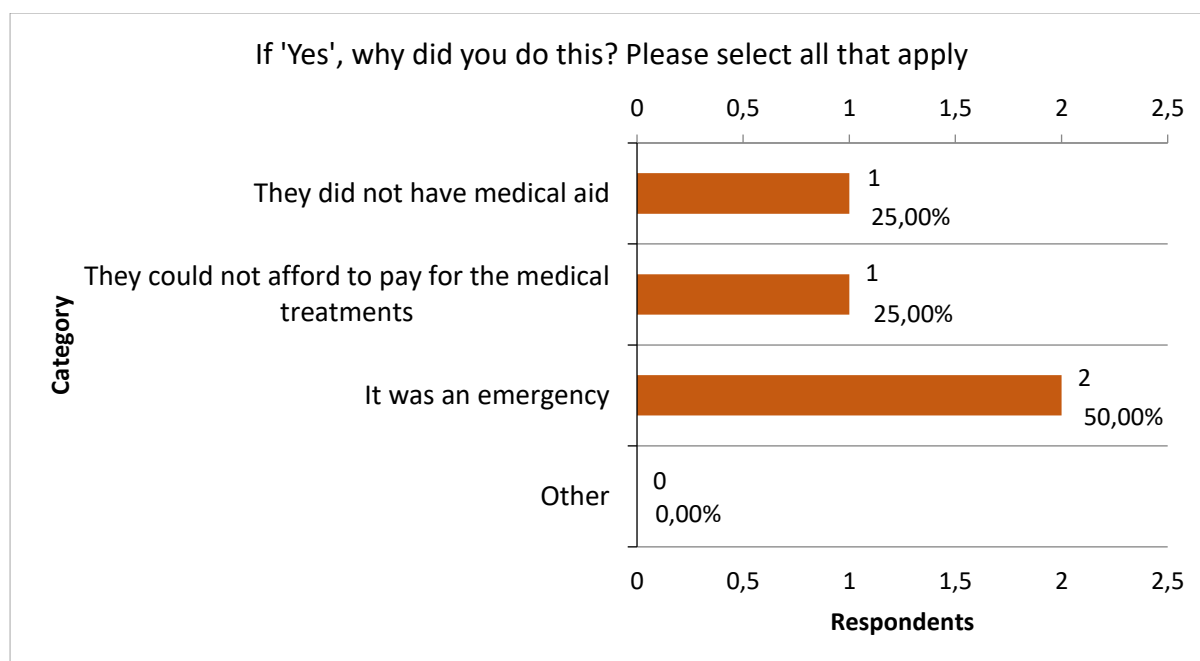


Figure 3.28: Reasons for Permitting Non-Family to Use Personal Identity

Figure 3.28 refers to three respondents, determining their reason for sharing personal identity with another individual who is not a family member. The results are as follows:

- 1 (25.00%) respondents selected 'They did not have medical aid'.
- 1 (25.00%) respondents selected 'They could not afford to pay for the medical treatment'.
- 2 (50.00%) respondents selected 'It was an emergency'.
- 0 (0.00%) respondent selected 'Other'.

From the three respondents, the results show that about 50% indicated sharing personal identity was for an emergency, while one (25%) respondent indicated not having medical aid as a reason. The other one (25%) respondent indicated that the treatment was too expensive, so they offered their personal identity to help out another individual. This could be that South African felt the need to help individuals they know who are close friends with medical aid assistance, even though these were not family members.

3.7.6 If 'Yes', how often did you share your personal healthcare information?

This question identified how often the respondents allowed their personal identity to be shared with other individuals.

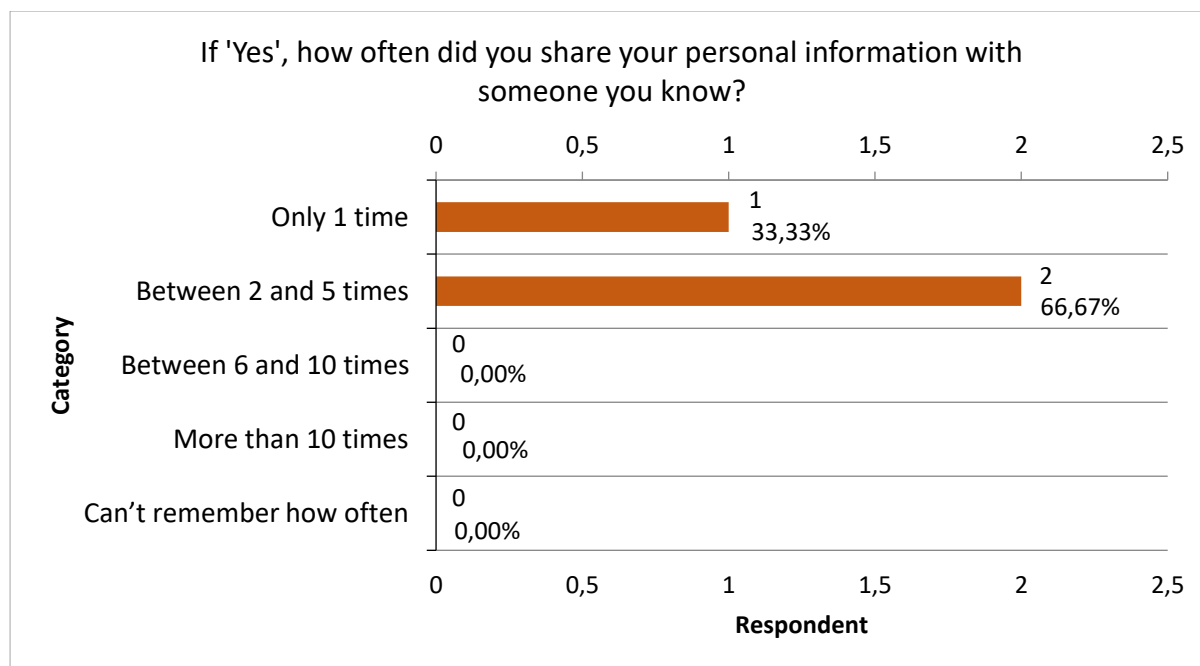


Figure 3.29: Frequency of Helping Non-Family Members

Figure 3.29 refers to three respondents. It indicates how frequently the respondent personal identity was shared with another individual who is not a family member. The results are as follows:

- 1 (33.33%) respondent selected 'Only 1 time'.
- 2 (66.67%) respondents selected 'Between 2 and 5 times'.
- 0 (00.00%) respondent selected 'Between 6 and 10 times'.
- 0 (00.00%) respondent selected 'More than 10 times'.
- 0 (0.00%) respondent selected 'Can't remember how often'.

Two (66.67%) of the respondents identified they have shared their personal healthcare information with a non-family member between two to five times while one (33.33%) respondent shared it with another person only once.

3.7.7 Were you or someone a victim of medical identity theft

This question focuses on determining whether the respondents or close relatives had been a victim to medical identity theft. This question determined the experience the respondents had dealt with, which in turn impacted on the next question they proceeded to.

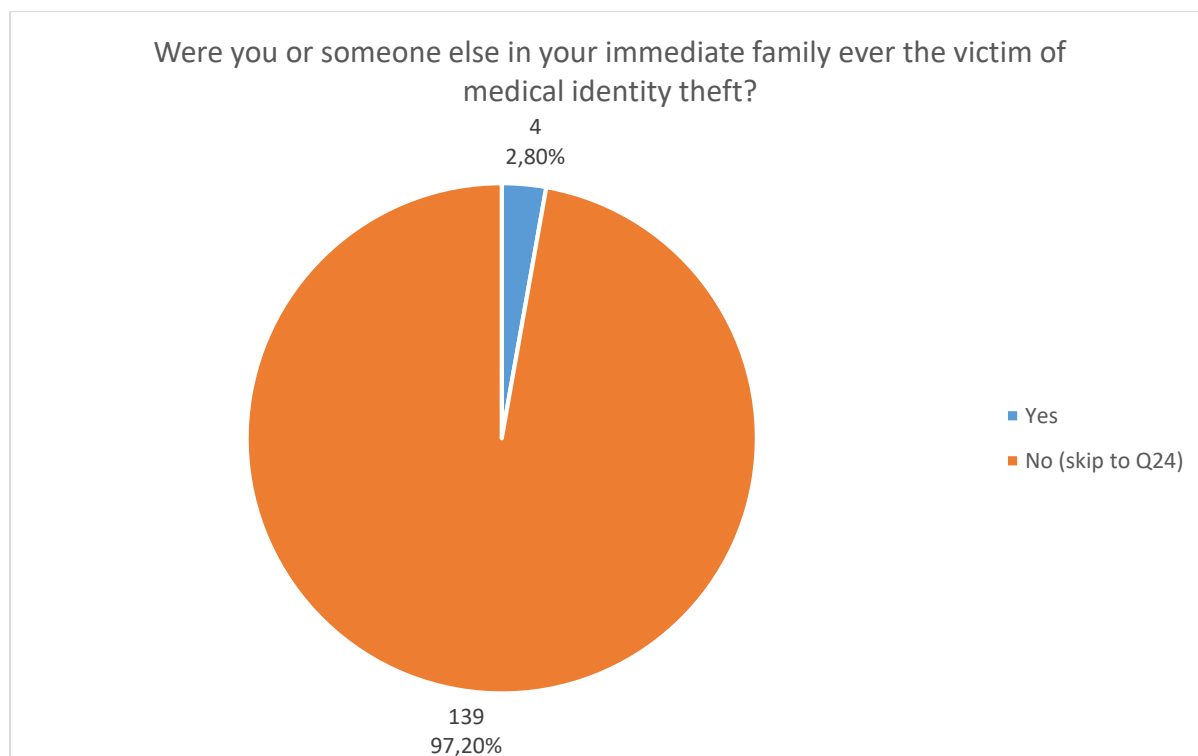


Figure 3.30: Do you Know Who is the Victims of Medical Identity Theft

Figure 3.30 relates to 143 respondents. It determines whether the respondents or close relatives have been a victim of medical identity theft. The results are as follows:

- 4 (2.80%) respondents selected 'Yes'.
- 139 (97.20%) respondents selected 'No'.

Four (2.80%) respondents indicated that they or someone in the immediate family had been a victim of medical identity theft. However, most of the respondents (97.20%) reported that they had not been directly impacted or did not know of someone in their family who had been a victim of medical identity theft.

Therefore, the following sections 3.7.8 to section 3.7.22 focussed specifically on the four respondents who selected the 'Yes' option. When the respondents had completed these questions, they joined the remaining 139 respondents who had selected the 'No' option and continued on section 3.7.23.

3.7.8 If 'Yes', who was the identity theft victim?

The question here identified who the victim was as mentioned in 3.7.7

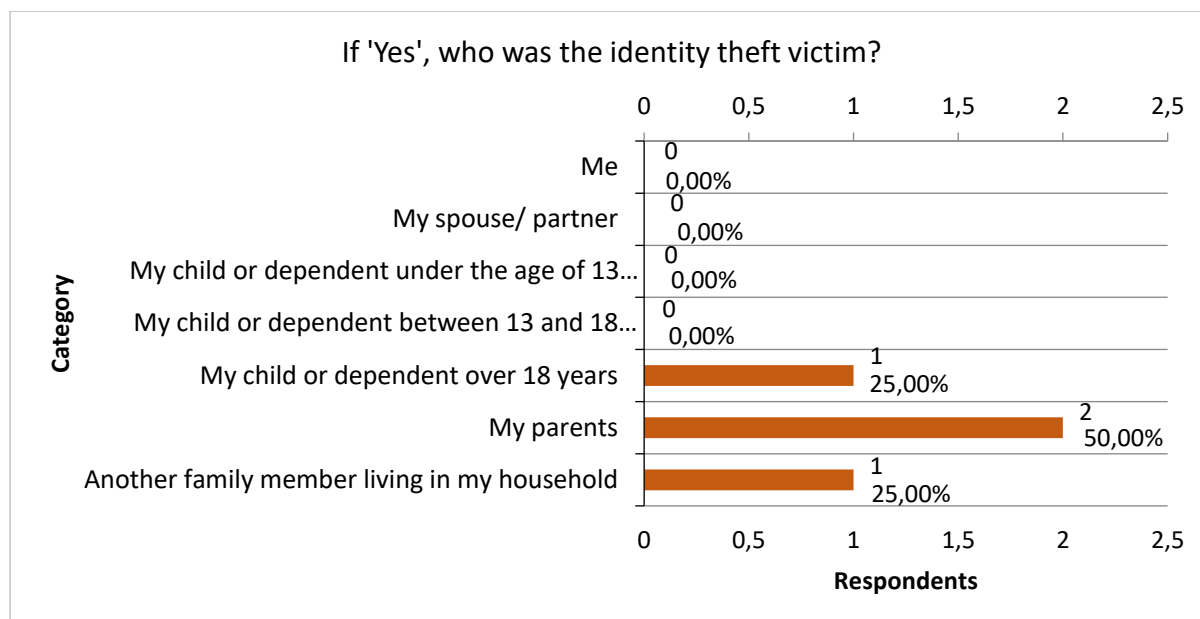


Figure 3.31: Who is the Victim of Medical Identity Theft

Figure 3.31 refers to four respondents. It determines who the medical identity theft victim was. The results are as follows:

- 0 (0.00%) respondent selected 'Me'.
- 0 (0.00%) respondent selected 'My spouse / partner'.
- 0 (0.00%) respondent selected 'My child or dependents under the age of 13 years'.
- 0 (0.00%) respondent selected 'My child or dependents between 13 and 18 years'.
- 1 (25.00%) respondent selected 'My child or dependents over 18 years'.
- 2 (50.00%) respondents selected 'My parents'.
- 1 (25.00%) respondent selected 'Another family member living in my household'.

The results show that those respondents who had been affected by medical identity theft were over 18 years old. One respondent indicated their child or a dependent over 18 years old had been affected. In addition, two respondents, which was the highest rate, identified their parents as the medical identity theft victims and one of the respondents selected that the victim was another family member living with them. No other respondents identified any other victims below 18 or had personal medical identity theft experience.

3.7.9 How would you describe your medical identity theft incident?

This question is aimed at understanding how the respondents' medical identity theft took place.

Chapter 3: Level of Awareness in the Private Healthcare Sector

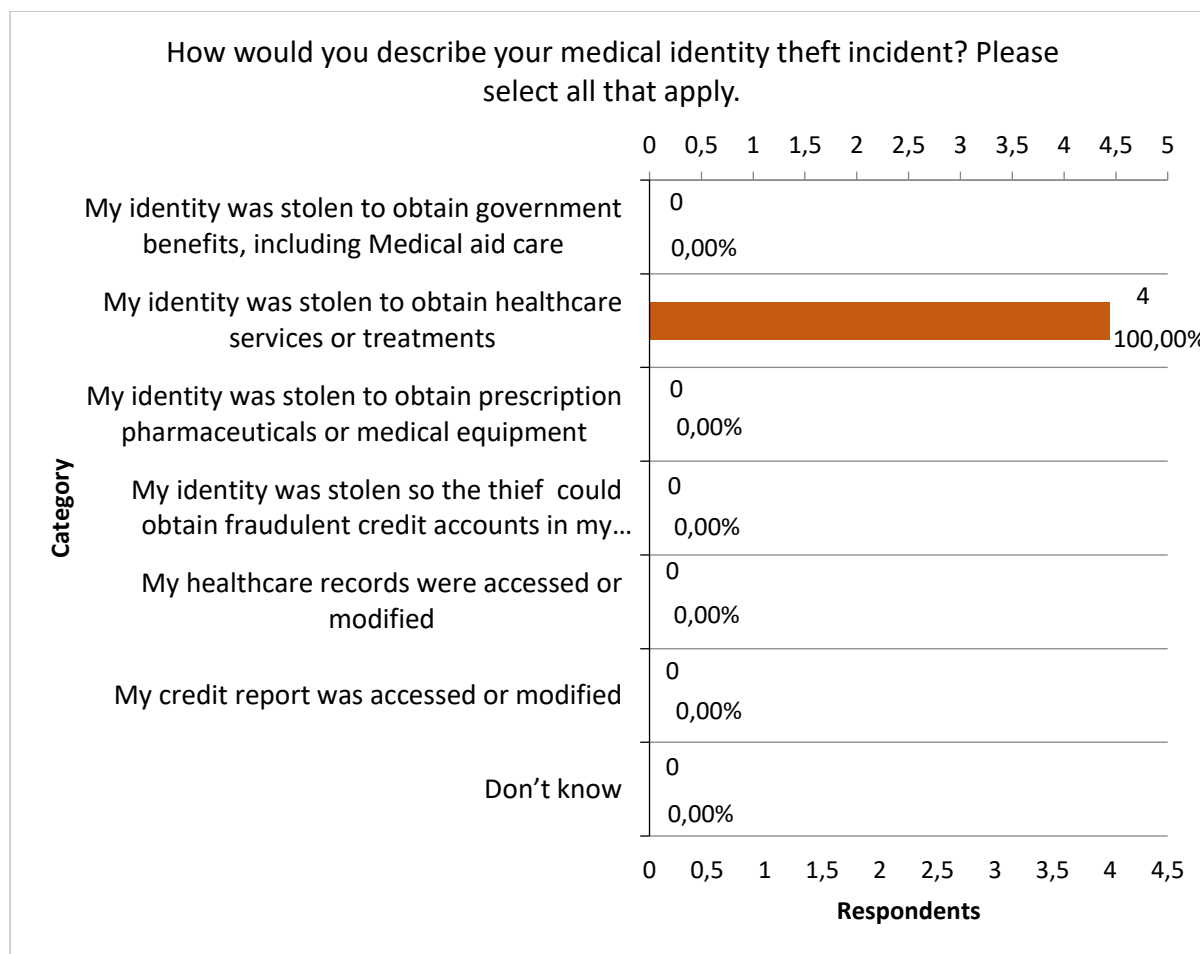


Figure 3.32: Type of Medical Aid Theft

Figure 3.32 refers to respondents. It determines how the respondents described their medical identity theft incident. The results are as follows:

- 0 (0.00%) respondent selected 'My identity was stolen to obtain government benefits, including medical aid care'.
- 4 (100.00%) respondents selected 'My identity was stolen to obtain healthcare services or treatments'.
- 0 (0.00%) respondent selected 'My identity was stolen to obtain prescription pharmaceutical or medical equipment'.
- 0 (0.00%) respondent selected 'My identity was stolen so the thief could obtain fraudulent credit accounts in my name'.
- 0 (0.00%) respondent selected 'My healthcare records were accessed or modified'.
- 0 (0.00%) respondent selected 'My credit reports was accessed or modified'.
- 0 (0.00%) respondent selected 'Don't know'.

From the four respondents, 100% indicated that their identity had been stolen for healthcare services or treatment.

3.7.10 How did you learn about medical identity theft?

This question aimed at finding out how respondents learned that they had been victims of medical identity theft. This question allowed respondents multiple selections.

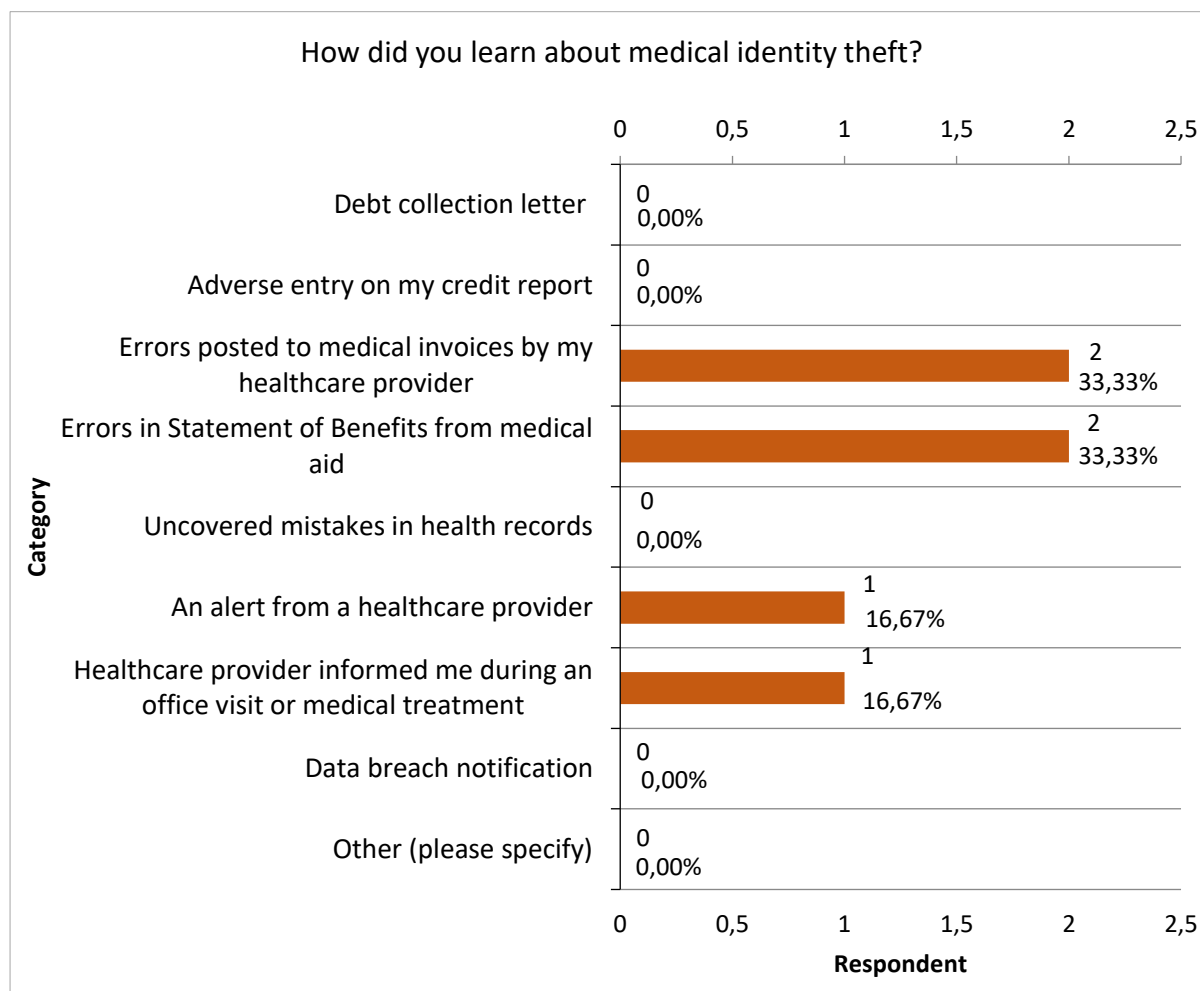


Figure 3.33: How Theft Was Detected

Figure 3.33 refers to four respondents. It determined how the respondents had learnt of medical identity theft. The results are as follows:

- 0 (0.00%) respondent selected 'Debt collection letter'.
- 0 (0.00%) respondent selected 'Adverse entry on my credit report'.
- 2 (33.33%) respondents selected 'Errors posted to medical invoices by my healthcare provider'.
- 2 (33.33%) respondents selected 'Error in statement of benefits from medical aid'.
- 0 (0.00%) respondent selected 'Uncovered mistakes in health records'.

Chapter 3: Level of Awareness in the Private Healthcare Sector

- 1 (16.67%) respondent selected 'An alert from healthcare provider'.
- 1 (16.67%) respondent selected 'Healthcare provider informed me during an office visit or medical treatment'.
- 0 (0.00%) respondent selected 'Data breach notification'.
- 0 (0.00%) respondent selected 'Other'.

The results shows that two category groups with equal response rates of 33.33% indicated error posted in the respondents' medical records from healthcare provider and errors in the statement of benefit from medical aid as the means by which they had learnt of the theft. The next highest response rate with 16.67% by two categories refer to alerts from a healthcare provider and the healthcare provider informing them during a visit or medical treatment of the medical identity theft incident.

3.7.11 When did you learn you were a victim of medical identity theft?

This question determined the time it took for the respondents to learn of the incident.

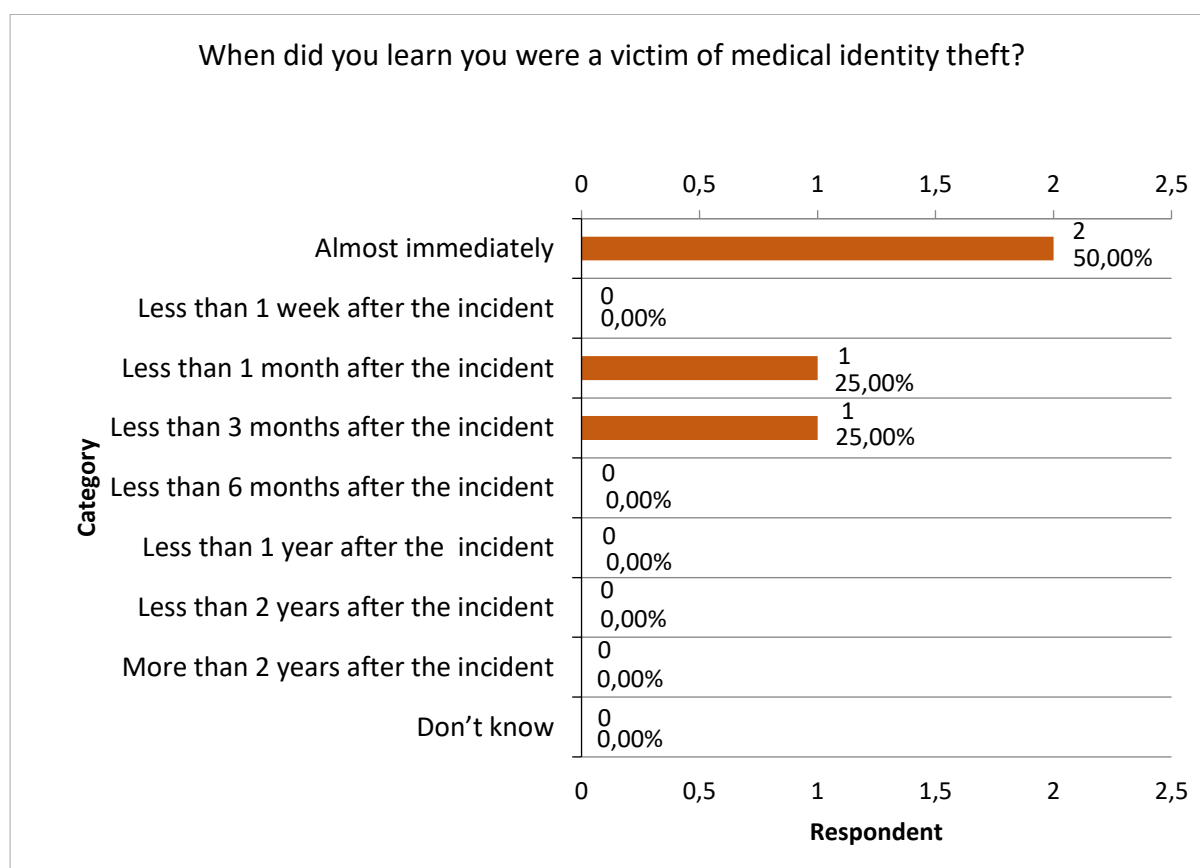


Figure 3.34: Length of Time to Discover Medical Identity Theft

Figure 3.34 refers to four respondents. It determined how long it took for them to find out about the incident. The results are as follows:

Chapter 3: Level of Awareness in the Private Healthcare Sector

- 2 (50.00%) respondents selected 'Almost immediately'.
- 0 (0.00%) respondent selected 'Less than 1 week after the incident'.
- 1 (25.00%) respondent selected 'Less than 1 month after the incident'.
- 1 (25.00%) respondent selected 'Less than 3 months after the incident'.
- 0 (0.00%) respondent selected 'Less than 6 months after the incident'.
- 0 (0.00%) respondent selected 'Less than 1 year after the incident'.
- 0 (0.00%) respondent selected 'Less than 2 years after the incident'.
- 0 (0.00%) respondent selected 'More than 2 years after the incident'.
- 0 (0.00%) respondent selected 'Don't know'.

The results indicate that 2 (50%) of the respondents learn of the medical identity theft almost immediately. In addition, one respondent took less than one month to find out while the other respondent took longer, namely less than three months.

This could point to the fact that not many SA medical aid members check their medical records or statement of benefits.

3.7.12 Once you became aware, did you report the incident?

This question determined whether the respondents took the initiative to report the incident immediately to officials or a legal individual.

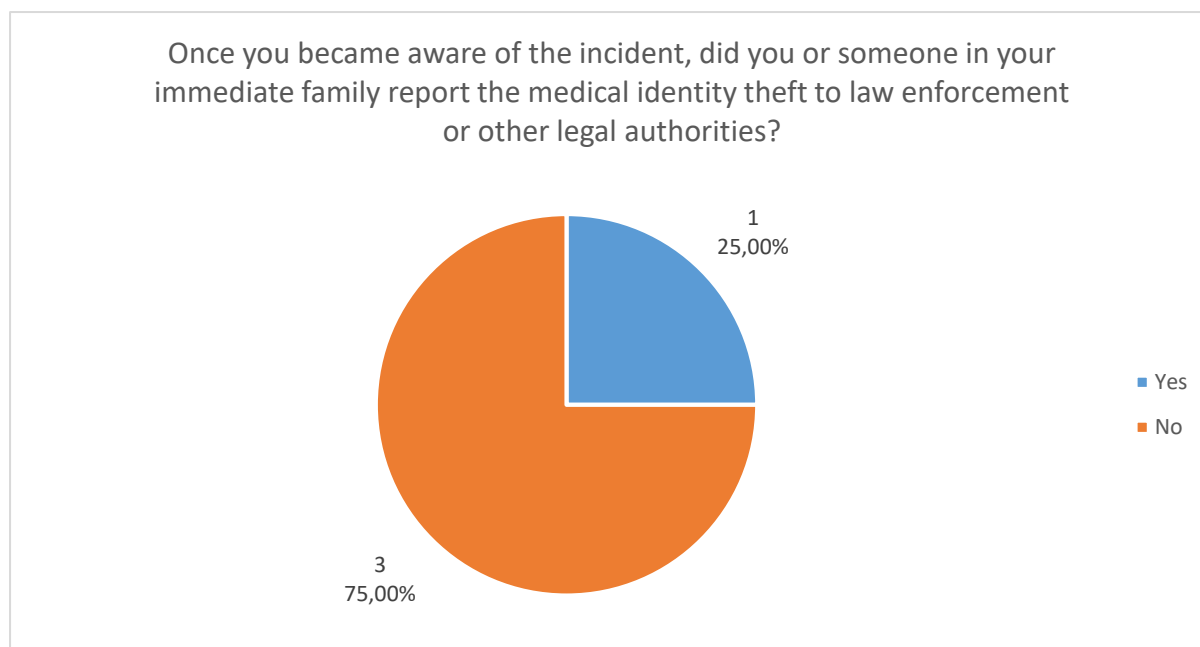


Figure 3.35: Report of Incidence of Medical Identity Theft

Figure 3.35 refers to four respondents. It determined whether this incident had been reported to any law officials. The results are as follows:

Chapter 3: Level of Awareness in the Private Healthcare Sector

- 1 (25.00%) respondent selected 'Yes'.
- 3 (75.00%) respondents selected 'No'.

Three respondents indicated that neither they nor a close relative had informed any officials of the situation. Only one of the respondents reported the incident.

The three respondents who had selected 'No', were transferred to section 3.7.13, The remaining respondent who had selected the 'Yes' option continued to 3.7.14, where they were later joined by the other three respondents.

3.7.13 If 'No', why was the medical identity theft not reported?

Based on the previous responses if the respondents had selected 'No' for not reporting medical identity theft incident to officials such as law enforcements or legal authorities, then the question here identified the reason why the incident had not been reported. This question allows respondents with multiple selections.

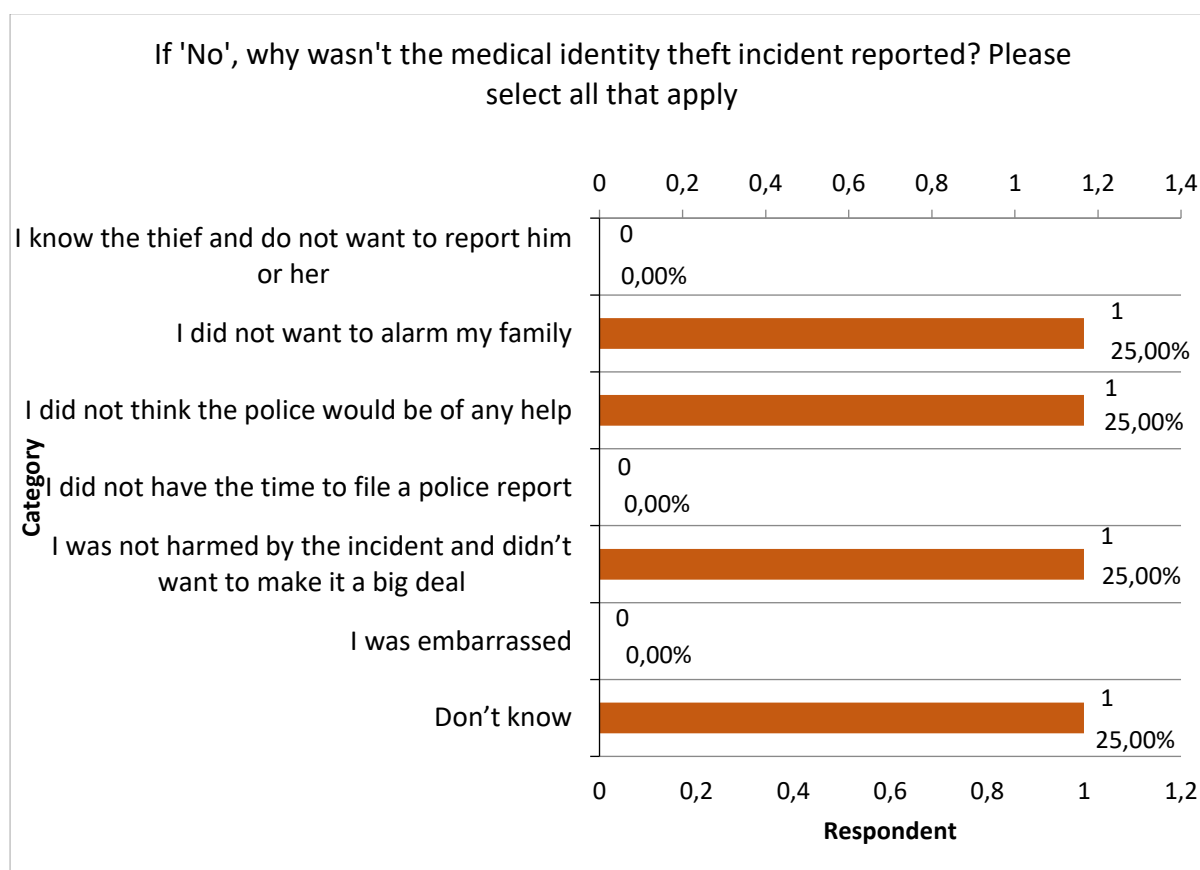


Figure 3.36: Reasons Why Medical Identity Theft Was Not Reported

Figure 3.36 refers to three respondents. It identifies why they had not reported the incident to officials. The results are as follows:

Chapter 3: Level of Awareness in the Private Healthcare Sector

- 0 (0.00%) respondent selected 'I know the thief and do not want to report him or her'.
- 1 (25.00%) respondent selected 'I did not want to alarm my family'.
- 1 (25.00%) respondent selected 'I did not think the police would be of any help'.
- 0 (0.00%) respondent selected 'I did not have the time to file a police report'.
- 1 (25.00%) respondent selected 'I was not harmed by the incident and didn't want to make it a big deal'.
- 0 (0.00%) respondent selected 'I felt embarrassed'.
- 1 (25.00%) respondent selected 'Don't know'.

Each respondent selected four major categories, namely not alarming family members, thinking that the police would not be any assistance, and no harm being caused. Lastly, the respondent did not know to whom to report the incident.

This could show that the respondents are unsure who can assist in issues such as medical identity theft. In addition, they believe they could not rely on the assistance from police.

3.7.14 How did the medical identity theft happen

This question is based on the respondents' knowledge of how medical identity theft occurred. This question required users to select the mostly likely cause.

Chapter 3: Level of Awareness in the Private Healthcare Sector

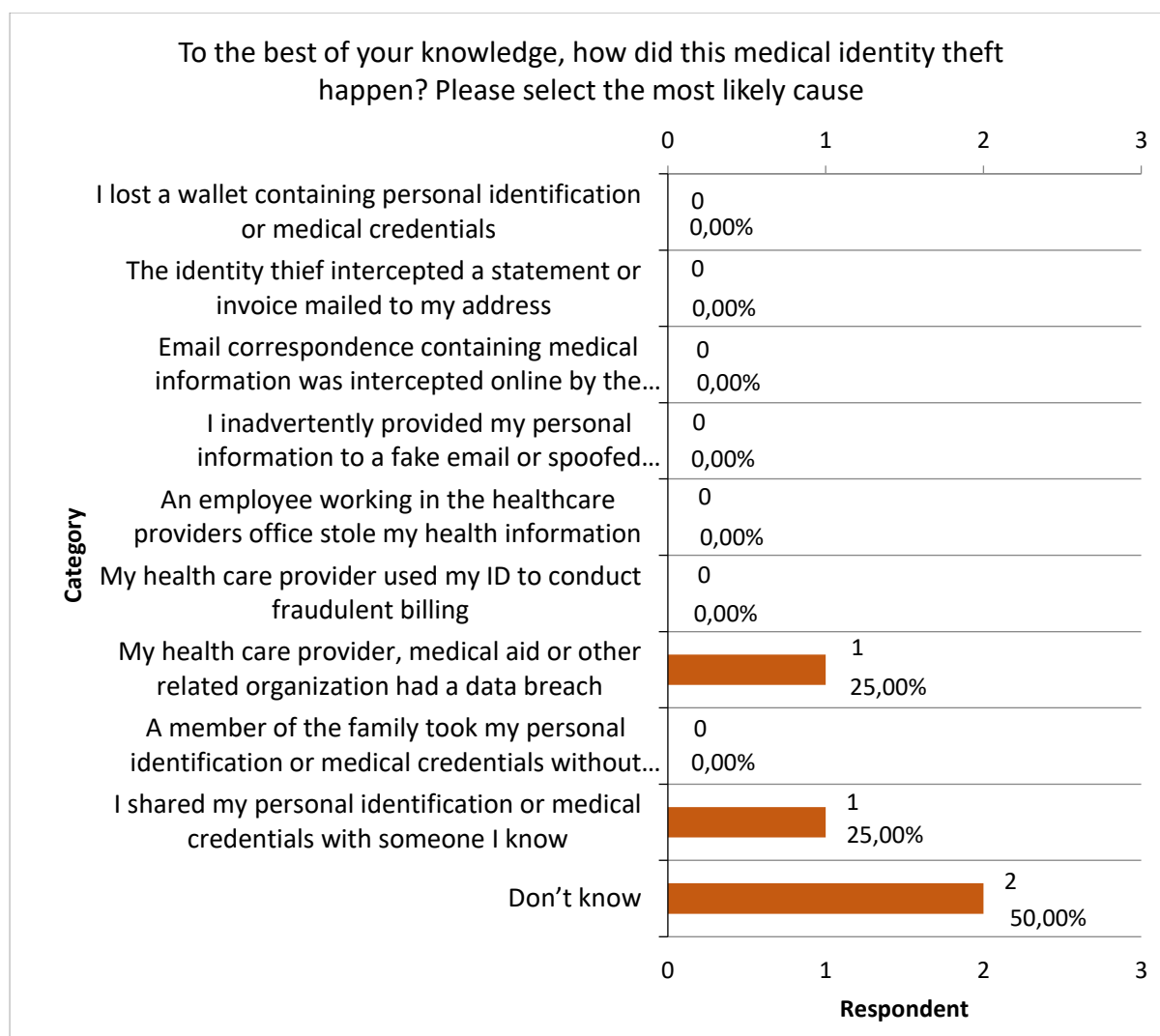


Figure 3.37: Details of Occurrence of Medical Aid Theft

Figure 3.37 refers to four respondents who were asked to select the most likely cause as to how medical identity theft happened. The results are as follows:

- 0 (0.00%) respondent selected 'I lost a wallet containing personal identification or medical credentials'.
- 0 (0.00%) respondent selected 'The identify theft intercepted a statement or invoice mailed to my address'.
- 0 (0.00%) respondent selected 'Email correspondence containing medical information was intercepted online by the identity thief'.
- 0 (0.00%) respondent selected 'I inadvertently provided my personal information to a fake email or spoofed website'.
- 0 (0.00%) respondent selected 'An employee working in the healthcare providers' office stole my health information'.

Chapter 3: Level of Awareness in the Private Healthcare Sector

- 0 (0.00%) respondent selected 'My healthcare provider used my ID to conduct fraudulent billing'.
- 1 (25.00%) respondent selected 'My healthcare provider, medical aid or other related organization had a data breach'.
- 0 (0.00%) respondent selected 'A member of the family took my personal identification or medical credentials without my consent'.
- 1 (25.00%) respondent selected 'I shared personal identification or medical credentials with someone they know'.
- 2 (50.00%) respondents selected 'Don't know'.

Two (50%) of the respondents indicated that they did not know how their medical identity theft had occurred. One respondent indicated the theft occurred due to a data breach and the remaining respondent had allowed their identity to be shared.

3.7.15 What were the financial consequences of medical identity theft incident?

This question gauges the impact of the financial consequences of medical identity theft on the respondents. This question allows for two choices by respondents.

Chapter 3: Level of Awareness in the Private Healthcare Sector

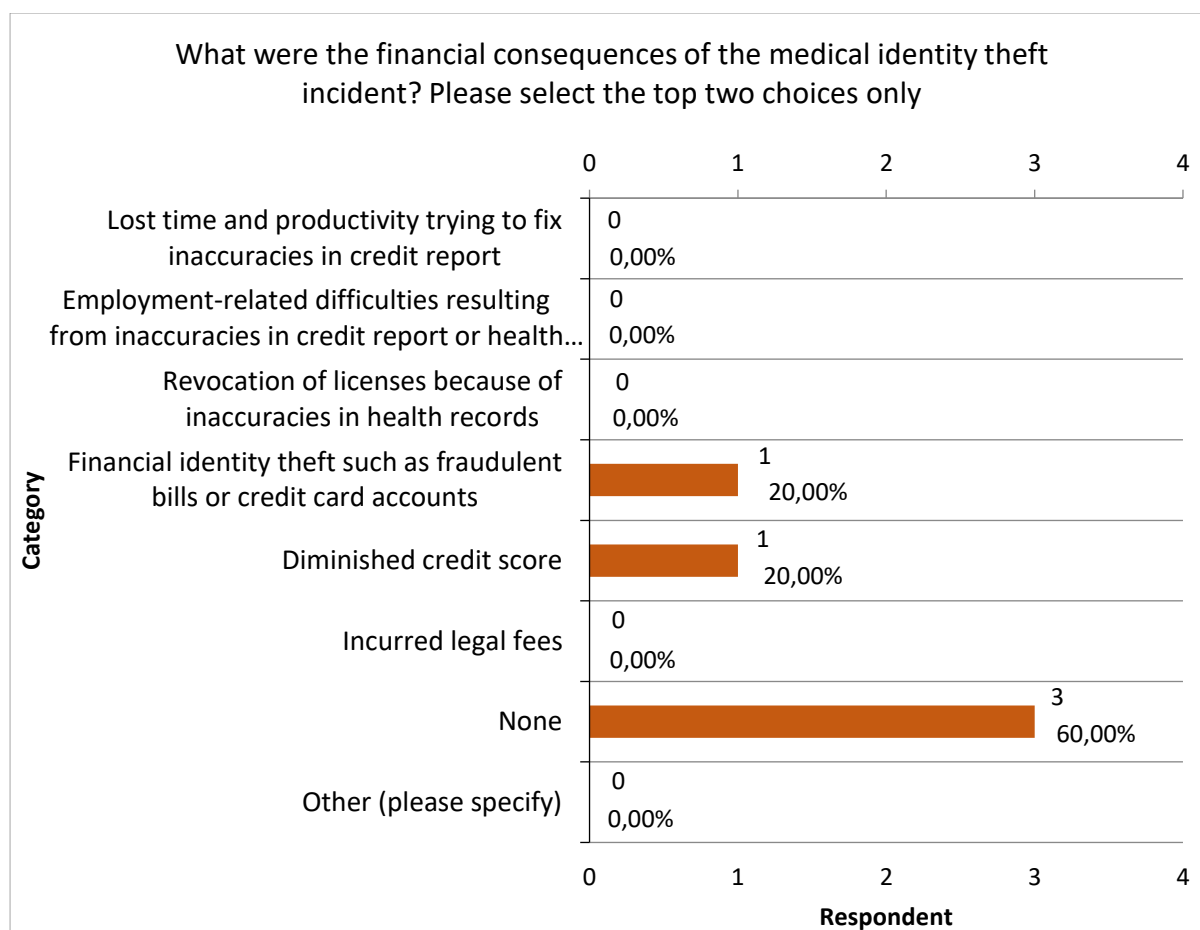


Figure 3.38: Financial Consequences of Medical Identity Theft

Figure 3.38 refers to four respondents. It identified the financial consequences of medical identity theft. The results are as follows:

- 0 (0.00%) respondent selected ‘Lost time and productivity trying to fix inaccuracies in credit report’.
- 0 (0.00%) respondent selected ‘Employment-related difficulties resulting from inaccuracies in credit report or health records’.
- 0 (0.00%) respondent selected ‘Revocation of licenses because of inaccuracies in health records’.
- 1 (20.00%) respondent selected ‘Financial identity theft such as fraudulent bills or credit card accounts’.
- 1 (20.00%) respondent selected ‘Diminished credit score’.
- 0 (0.00%) respondent selected ‘Incurred legal fees’.
- 3 (60.00%) respondents selected ‘None’.
- 0 (0.00%) respondent selected ‘Other’.

Three respondents, who indicated that they had incurred no financial consequences from medical identity theft. In addition, a respondent mentioned financial identity theft from bills and credit cards and their credit score had dropped owing to medical identity theft.

Victims of medical identity theft face issues such as diminished credit records and financial identity theft when they are not aware of the occurrence of the theft. If they had known, they could have taken steps in order to quickly resolve this issue.

3.7.16 What were the medical consequences of medical identity theft incident?

This question determined whether the respondents had any medical consequences of medical identity theft. This question allowed for two top choices by respondents.

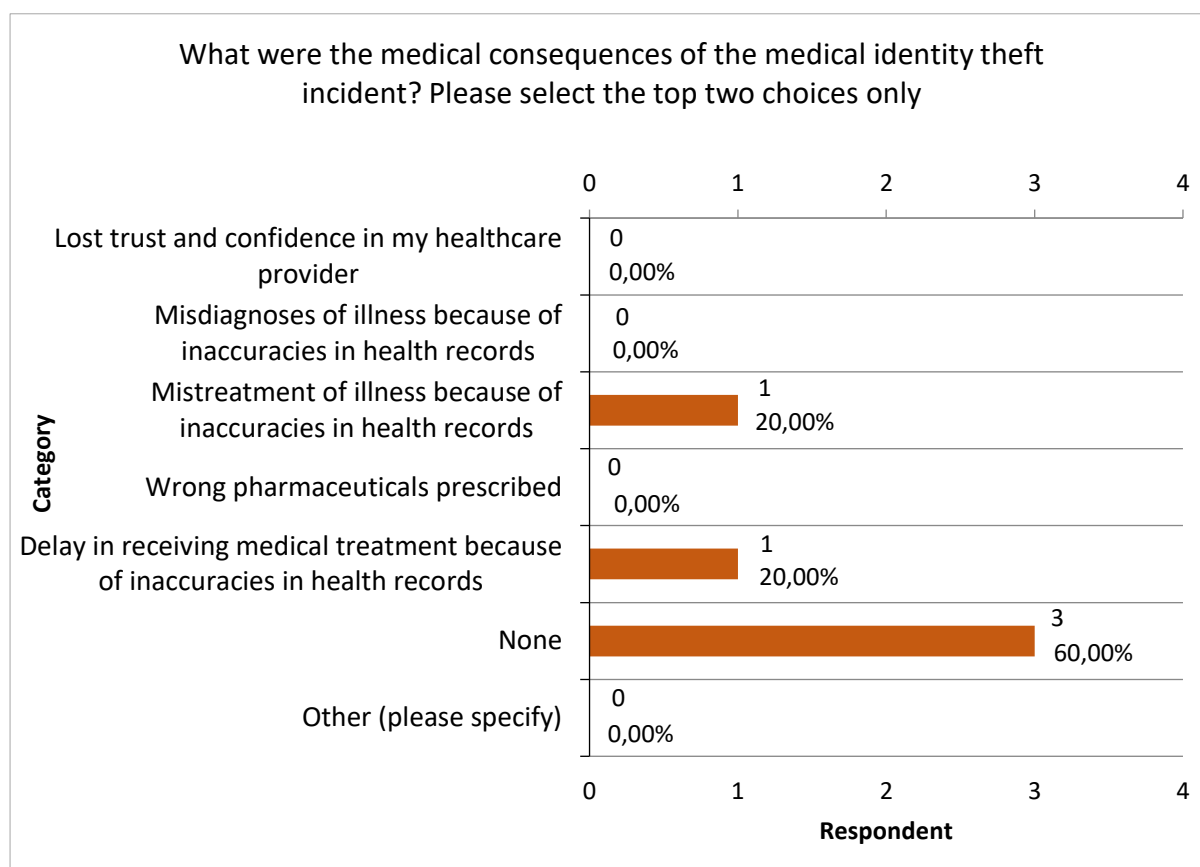


Figure 3.39: Medical Consequences of Medical Identity Theft

In Figure 3.39, consist of 4 respondents, identifies the medical care impact which medical identity theft has left the respondents facing. The results are as follows:

- 0 (0.00%) respondent selected 'Lost trust and confidence in my healthcare provider'.
- 0 (0.00%) respondent selected 'Misdiagnoses of illness because of inaccuracies in health records'.

Chapter 3: Level of Awareness in the Private Healthcare Sector

- 1 (20.00%) respondent selected 'Mistreatment of illness because of inaccuracies in health records'.
- 0 (0.00%) respondent selected 'Wrong pharmaceuticals prescribed'.
- 1 (20.00%) respondent selected 'Delay in receiving medical treatment because of inaccuracies in health records'.
- 3 (60.00%) respondents selected 'None'.
- 0 (0.00%) respondent selected 'Other'.

A respondent from section 3.7.24 indicated the following:

"Would cause financial strain and inaccurate medical history"

The respondent identified that financial strain and inaccurate medical history could be problematic, leading to possible mistreatment, misdiagnoses and delay in healthcare service. This indicates this respondent's awareness of medical identity theft and the impact it can cause on their records and personal finance.

3.7.17 What were the medical aid consequences of medical identity theft incident?

This question determined whether the respondent had any medical aid consequences regarding medical identity theft. This question allows for two top choices by respondents.

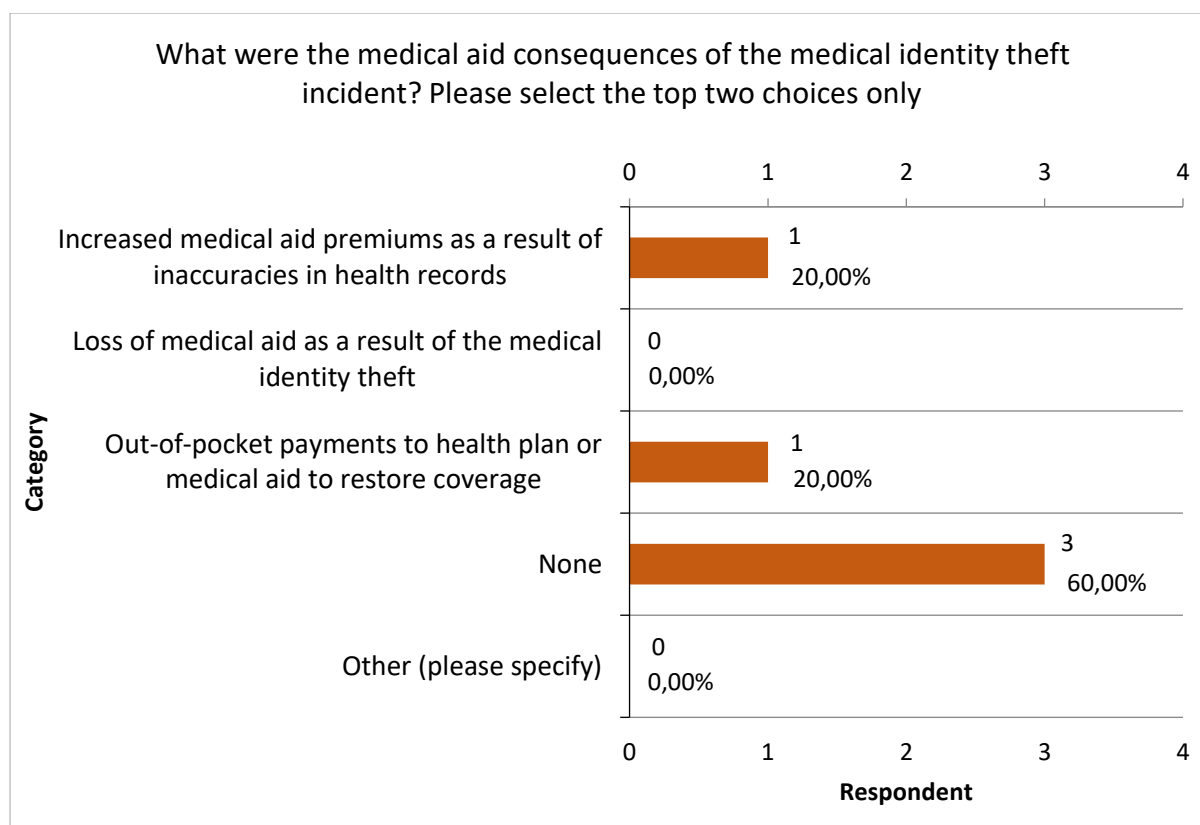


Figure 3.40: Medical Aid Consequences of Medical Identity Theft

Figure 3.40 refers to four respondents. It determined the medical aid impact of medical identity theft. The results are as follows:

- 1 (20.00%) respondent selected 'Increased medical aid premiums as a result of inaccuracies in health records'.
- 0 (0.00%) respondent selected 'Loss of medical aid as a result of the medical identity theft'.
- 1 (20.00%) respondent selected 'Out-of-pocket payments to health plan or medical aid to restore coverage'.
- 3 (60.00%) respondents selected 'None'.
- 0 (0.00%) respondent selected 'Other'.

Three respondents who indicated that they faced no medical aid consequences from medical identity theft. In addition, a respondent identified increase medical aid premiums as a result of inaccurate health records and reported that they were out of pocket owing to restoring the coverage owed to the medical aid.

3.7.18 Did you or your immediate family resolve the identity theft incident?

This question determined whether the respondents or any close relative had tried to resolve the medical identity theft.

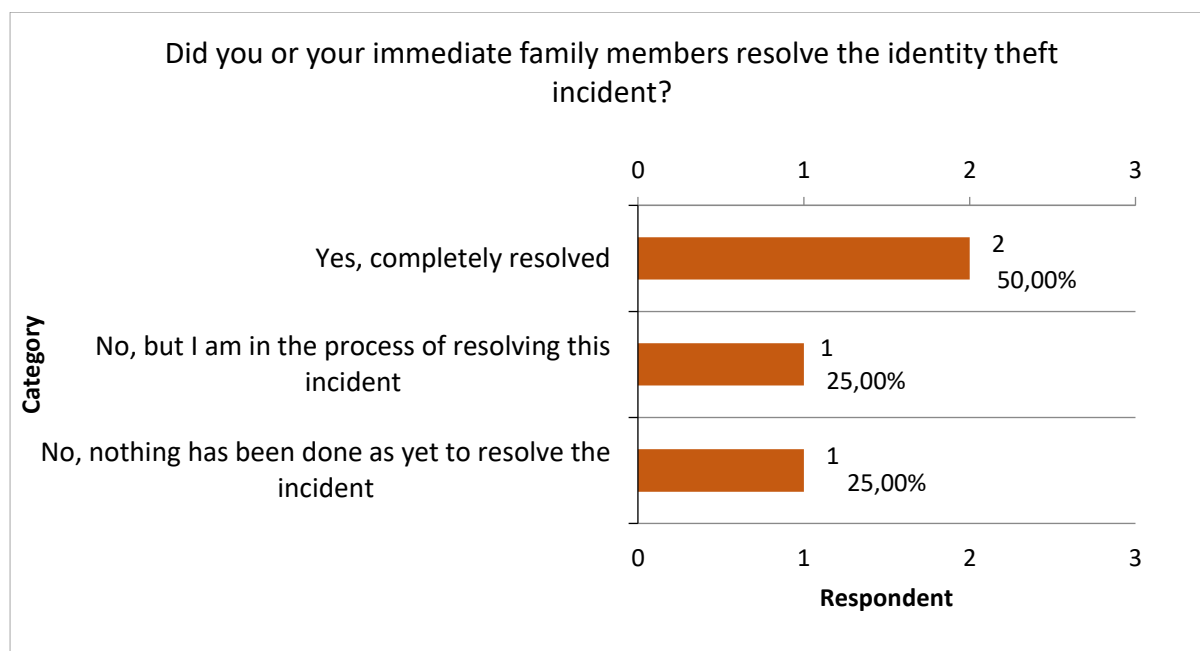


Figure 3.41: Resolving the Medical Identity Theft Incident

Figure 3.41 relates to four respondents, determining whether they or family member had tried to rectify the problem of medical identity theft immediately. The results are as follows:

- 2 (50.00%) respondents selected 'Yes, completely resolved'.
- 1 (25.00%) respondent selected 'No, but in the process of resolving the incident'.
- 1 (25.00%) respondent selected 'No, nothing has been done as yet to resolve the incident'.

Two of the respondents indicated that the incident of the medical identity theft had been rectified and completed fixed. In addition, a respondent indicated they were still in the process of resolving the issue of medical identity theft. The other respondents had done nothing to fix the issue.

The respondents who had not yet resolved the incident or were still in the process of doing so are not possibly fully aware of who to inform or notify. Chapter 4 discusses the officials who can be notified and informed of these incidents.

A total of two respondents who selected 'Yes', were transferred to sections 3.7.19 and 3.7.20 and were later joined by the remaining two at 3.7.21.

3.7.19 If 'Yes', how did you resolve this medical identity theft?

Based on the previous question, if the respondent selected 'Yes' for completely resolving the issue, then this question here identifies how the medical identity theft incident was resolved. This question allows respondents multiple selections.

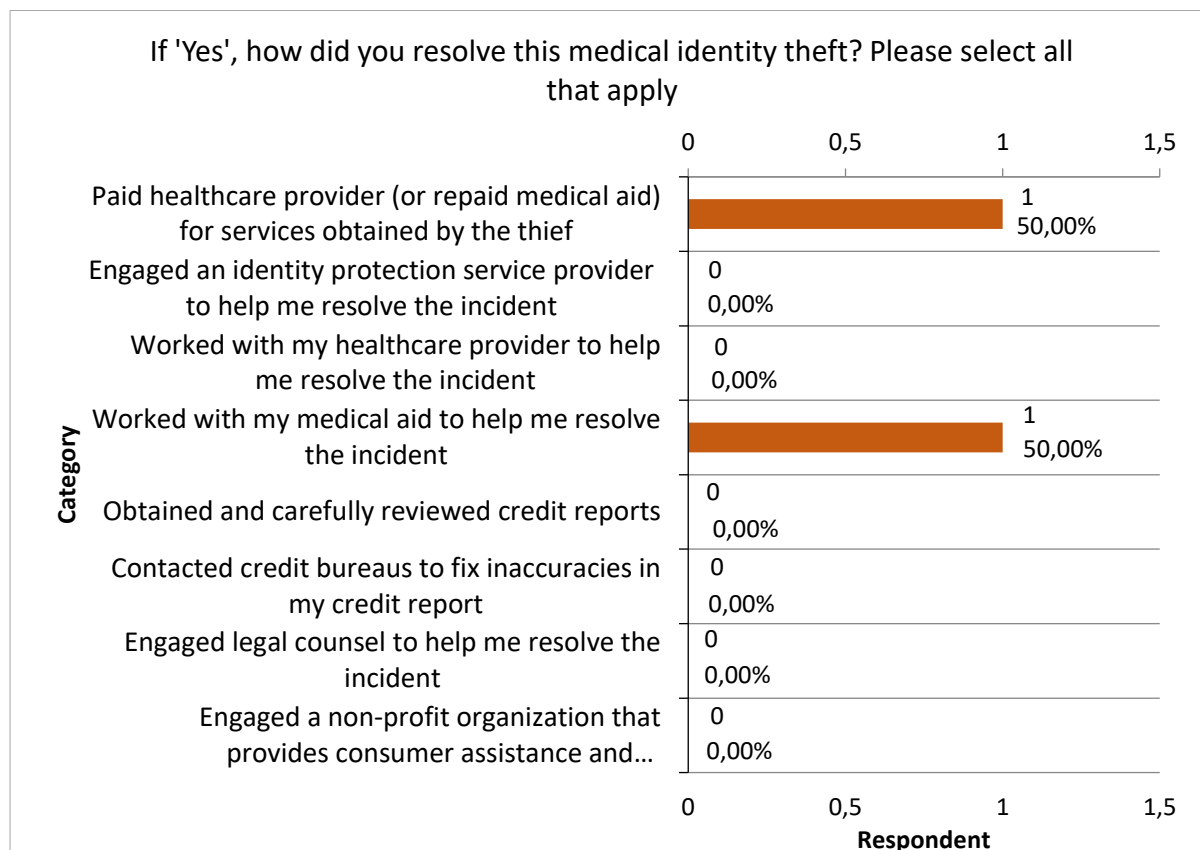


Figure 3.42: How Medical Identity Theft was Resolved

Figure 3.42 refers to two respondents. It identified how the medical identity theft was rectified. The results are as follows:

- 1 (50.00%) respondent selected 'Paid healthcare provider (or repaid medical aid) for services obtained by the thief'.
- 0 (0.00%) respondent selected 'Engaged an identity protection service provider to help me resolve the incident'.
- 0 (0.00%) respondent selected 'Worked with my healthcare provider to help me resolve the incident'.
- 1 (50.00%) respondent selected 'Worked with my medical aid to help me resolve the incident'.
- 0 (0.00%) respondent selected 'Obtained and carefully reviewed credit reports'.

Chapter 3: Level of Awareness in the Private Healthcare Sector

- 0 (0.00%) respondent selected 'Contacted credit bureaus to fix inaccuracies in my credit report'.
- 0 (0.00%) respondent selected 'Engaged legal counsel to me resolve the incident'.
- 0 (0.00%) respondent selected 'Engaged a non-profit organization that provides consumer assistance and support' (such as the South Africa Fraud Prevention Service).

Two of the respondents paid the healthcare provider or repaid the medical aid for the service obtained by the thief. The other two respondents worked with the medical aid to resolve the issue.

3.7.20 If 'Yes', how long did resolving the medical identity theft take?

Based on the response to section 3.7.18 if the respondent selected 'Yes' for completely resolving the issue, then this question would identify how long it took for the medical identity theft incident to be resolved.

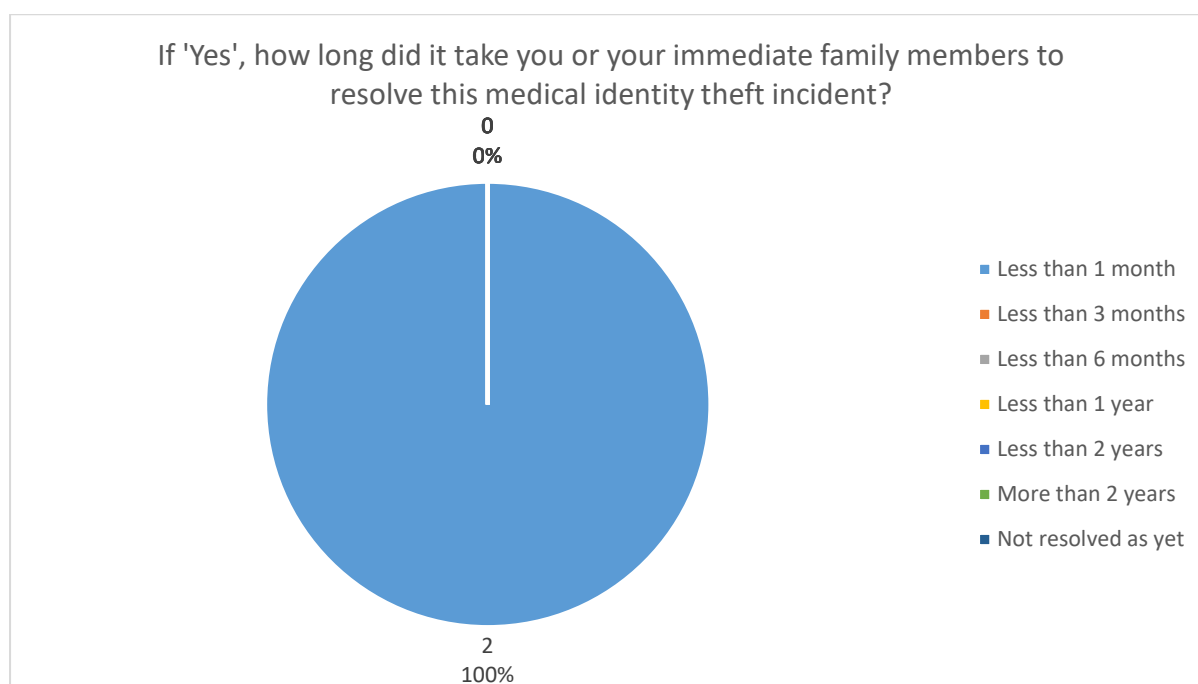


Figure 3.43: Length of Time to Resolve Incident

Figure 3.43 refers to two respondents. It identified how long it took to rectify the medical identity theft. The results are as follows:

- 2 (100.00%) respondents selected 'Less than 1 month'.
- 0 (0.00%) respondent selected 'Less than 3 months'.
- 0 (0.00%) respondent selected 'Less than 6 months'.

Chapter 3: Level of Awareness in the Private Healthcare Sector

- 0 (0.00%) respondent selected 'Less than 1 year'.
- 0 (0.00%) respondent selected 'Less than 2 years'.
- 0 (0.00%) respondent selected 'More than 2 years'.
- 0 (0.00%) respondent selected 'Not resolved as yet'.

All (100%) of the respondents indicated it took them less than one month to rectify the issue with medical identity theft.

3.7.21 Cost incurred trying to resolve medical identity theft

This question relates to three questions (Q22a to Q22c), which are depicted in the clustered charts. These represented the cost incurred by medical identity theft in three areas of focus; firstly, the money spent on identity theft protection, credit reporting and legal counsel; secondly, all out-of-pocket costs for medical services and medications because of the lapse in healthcare coverage; and thirdly, the reimbursements of healthcare providers to pay for services provided to imposters.

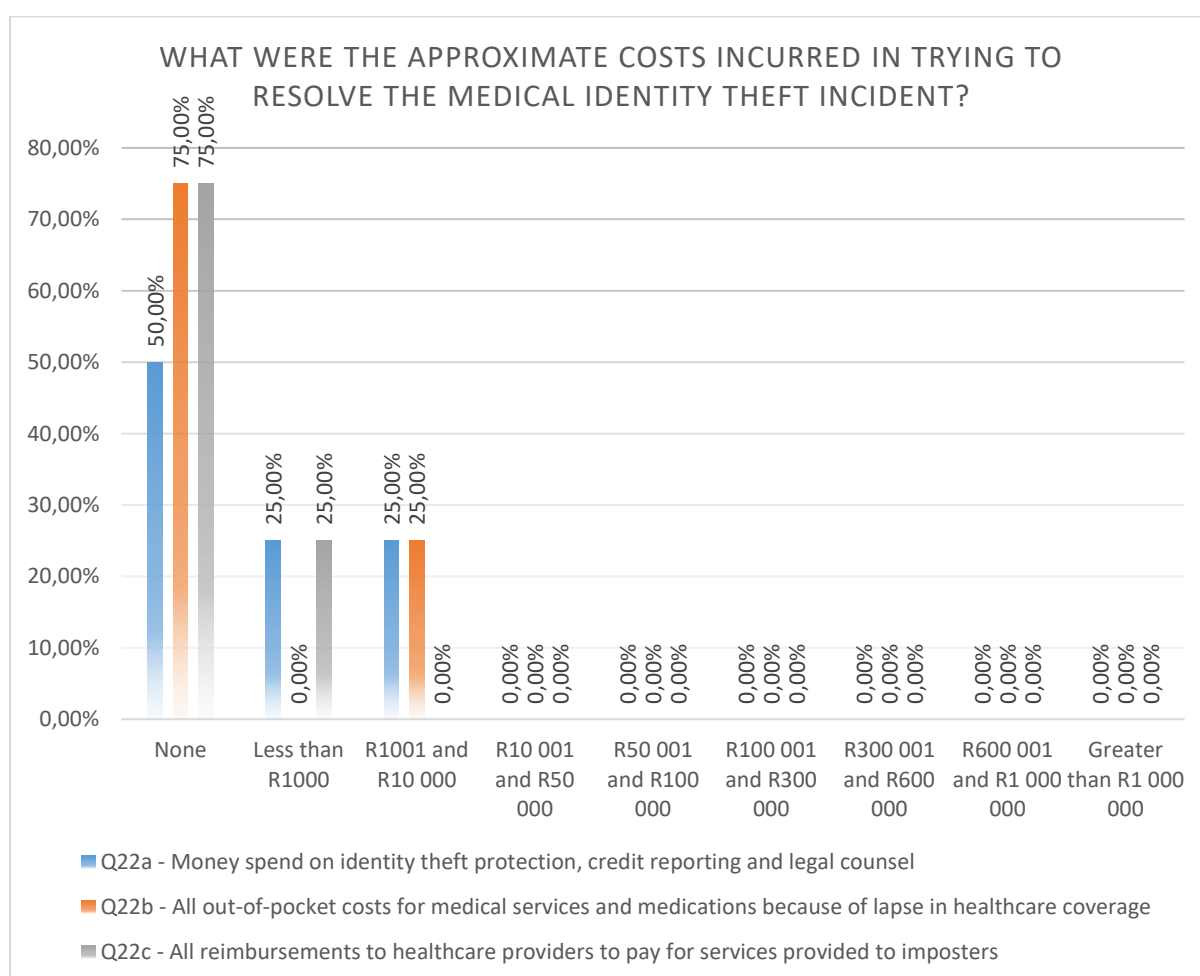


Figure 3.44: The Approximate Cost of Resolving Incidence of Medical Aid Theft

Chapter 3: Level of Awareness in the Private Healthcare Sector

Figure 3.44 relates to four respondents. The overall purpose of the question is to gauge the cost incurred by medical identity theft. The results are as follows:

Table 3.2: Cost Incurred by Medical Identity Theft

	Q22a	Q22b	Q22c
None	2 (50.00%)	3 (75.00%)	3 (75.00%)
Less than R1000	1 (25.00%)	0 (0.00%)	1 (25.00%)
R1001 and R10 000	1 (25.00%)	1 (25.00%)	0 (0.00%)
R10 001 and R50 000	0 (0.00%)	0 (0.00%)	0 (0.00%)
R50 001 and R100 000	0 (0.00%)	0 (0.00%)	0 (0.00%)
R100 001 and R300 000	0 (0.00%)	0 (0.00%)	0 (0.00%)
R300 001 and R600 000	0 (0.00%)	0 (0.00%)	0 (0.00%)
R600 001 and R1 000 000	0 (0.00%)	0 (0.00%)	0 (0.00%)
Greater than R1 000 000	0 (0.00%)	0 (0.00%)	0 (0.00%)

The results depicted in Table 3.2 and Figure 3.44 identify the costs incurred per each question. The table indicates that more than 50% of the respondents did not incur any cost from medical identity theft, whether with identity protection, legal counsel, medical services or reimbursement to health providers.

However, two respondents had to pay for identity protection, credit reporting and legal counsel, amounting to between R1001 and R10 000. A respondents paid between R1001 and R10 000 for out of pocket payment for medical services and medication.

This shows that respondents tried to settle the damages incurred to regain their membership of the medical aid. However, certain respondents would rather pay for advice and support from officials in guiding them on how to proceed with medical identity theft.

3.7.22 How much time was spent trying to resolve medical identity theft incident?

This question identified the time spent on fixing the medical identity theft issue.

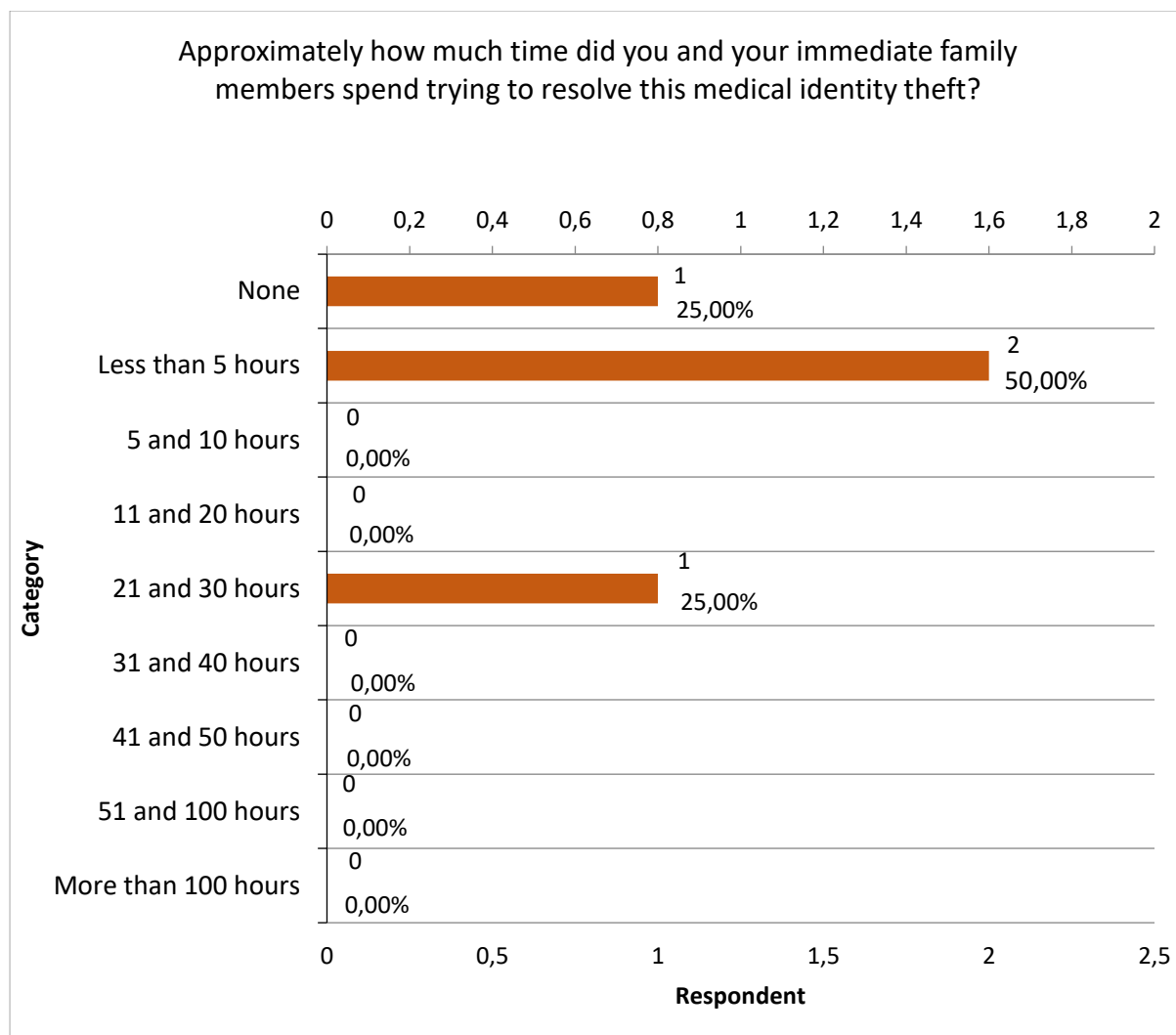


Figure 3.45: Time Spent on Resolving Issue of Medical Identity Theft

Figure 3.45 refers to four respondents. It identified the duration period taken to resolve the medical identity theft. The results are as follows:

- 1 (25.00%) respondent 'None'.
- 2 (50.00%) respondents selected 'Less than 5 hours'.
- 0 (0.00%) respondent selected '5 an 10 hours'.
- 0 (0.00%) respondent selected '11 an 20 hours'.
- 1 (25.00%) respondent selected '21 an 30 hours'.
- 0 (0.00%) respondent selected '31 an 40 hours'.
- 0 (0.00%) respondent selected '41 an 50 hours'.
- 0 (0.00%) respondent selected '51 an 100 hours'.
- 0 (0.00%) respondent selected 'More than 100 hours'.

Two respondents who identified less than five hours for the medical identity theft incident to be resolved. A respondents indicated 21 to 30 hours to resolve the issue, whereas the last respondent indicated that no time was required to resolve the medical identity incident.

The possible reason for the short time taken resolve the issue was that the respondent decided to settle the expenses of the perpetrator, therefore the medical identity theft expense was covered by the medical aid member.

3.7.23 Steps taken to prevent future medical identity theft incident

The following question identified the steps taken by the respondents or close relatives to prevent future medical identity theft incidents. This question allows the respondents to have multiple selections.

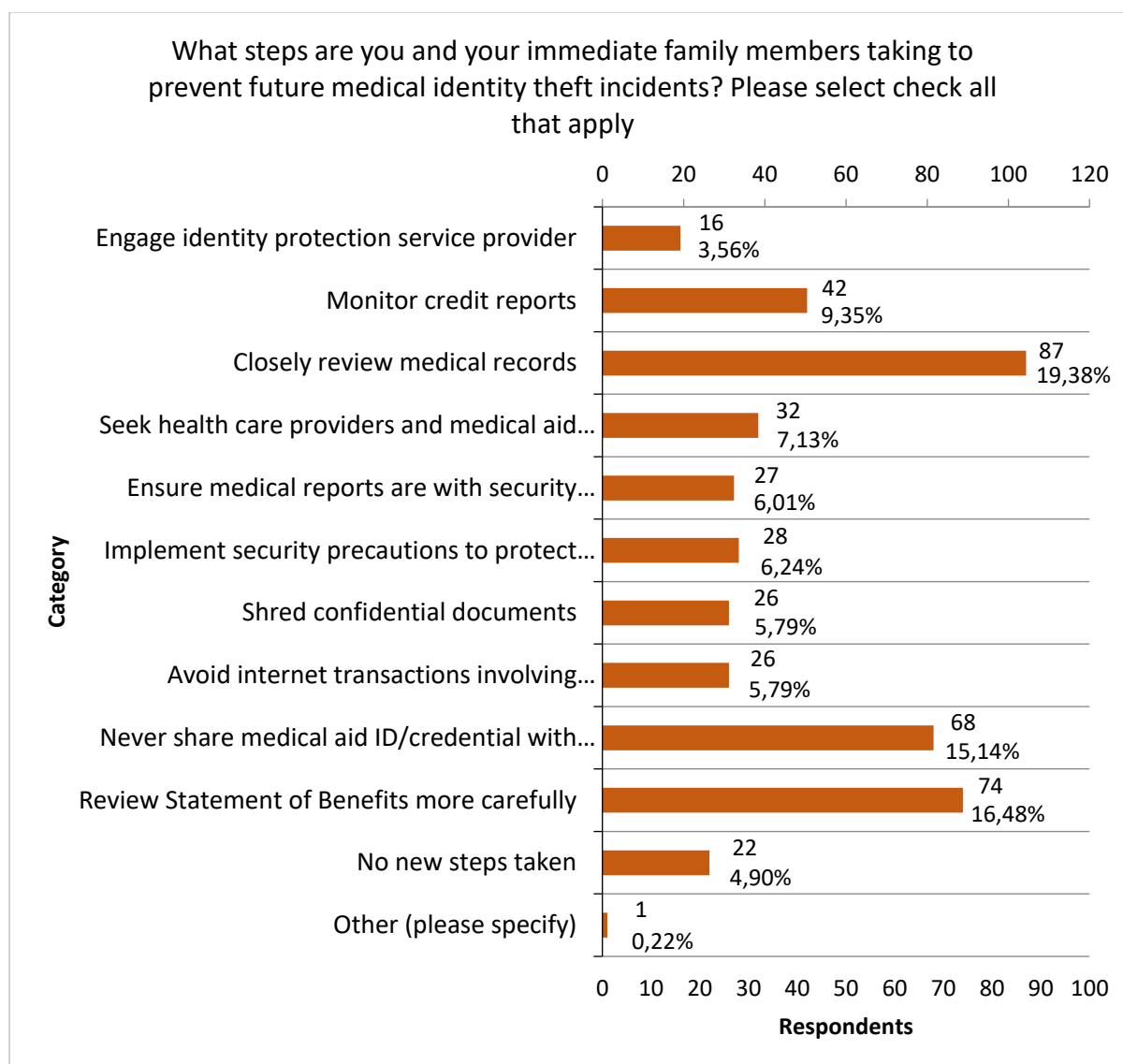


Figure 3.46: Steps to Avoid Future Medical Identity Theft

Chapter 3: Level of Awareness in the Private Healthcare Sector

Figure 3.46 refers to 143 respondents to determine the steps to be taken in future to prevent medical identity theft incidents occurring by the respondents or family members.

The results are as follows:

- 16 (3.56%) respondents selected 'Engage with identity protection service provider'.
- 42 (9.35%) respondents selected 'Monitor credit reports'.
- 87 (19.38%) respondents selected 'Closely review medical records'.
- 32 (7.13%) respondents selected 'Seek health care providers and insurers with better privacy and security practices'.
- 27 (6.01%) respondents selected 'Ensure medical reports are with security conscious vendors'.
- 28 (6.24%) respondents selected 'Implement security precautions to protect personal credentials'.
- 26 (5.79%) respondents selected 'Shred confidential documents'.
- 26 (5.79%) respondents selected 'Avoid internet transactions involving confidential information'.
- 68 (15.14%) respondents selected 'Never share medical aid ID/credential with anyone'.
- 74 (16.48%) respondents selected 'Review statement of benefits more carefully'.
- 22 (4.90%) respondents selected 'No new steps taken'.
- 1 (0.22%) respondent selected 'Other', as indicated below:

"I am a chronic patient so I deal with my medical aid almost every day"

The highest response rate of 19.38% refers to those who intend to closely review medical records. Reviewing their medical records allows the respondents to track whether any unauthorised use of the medical aid had been made. The next highest response rate is 16.48% reflecting those respondents who review statement of benefits carefully.

3.7.24 List any other issues or comments about medical identity theft

This open-ended question invites respondents to list any further issues or comments about medical identity theft.

Chapter 3: Level of Awareness in the Private Healthcare Sector

Of the 143 respondents, only 14 provided feedback, and eight responses were usable for verbatim quotes. The verbatim quotes as mentioned in section 3.2.1 are listed with the specific question.

The verbatim quotes indicate that the majority of the respondents were shocked and did not know that medical identity theft existed. After completing the survey the respondents felt they were more aware of medical identity theft. The comments provided indicated that this type of incident is an eye opener for many individuals who lack awareness.

The following section gives a brief summary of the survey results.

3.8 Summary

A survey was conducted with 216 respondents, of whom only 143 completed the questionnaire. A brief summary is provided of the five parts of the questionnaire:

Part 1 (demographics) found that the majority of the respondents are between the ages of 26 and 35 years old, with a large number of respondents from Gauteng Province. There was a slightly greater majority of female respondents, and all respondents were required to be current or former medical aid members.

Part 2 revealed that the majority of the respondents had not known of medical identity theft until participating in the survey. The way the respondents learnt of medical identity theft was from stories shared from friends and family members. Having prompt notification of medical identity theft was the most preferred option, and some respondents were not aware that medical identity theft can cause inaccuracies within their records.

Part 3 examines the issue of healthcare provider privacy, revealing that a third of the respondents do not check their medical records, as it had never occurred to them to actually check whether their medical records were correct. Some respondents merely reviewed records sent from the healthcare provider such as their SOBs. The respondents indicated securing medical records is important and if the healthcare provider was unable to protect medical records or breaches had to occur such as lost or stolen medical records, changing to another provider would be the next choice for the respondents.

Part 4 relating to medical aid privacy indicated that the majority of respondents are unsure whether their medical aid is concerned about medical identity theft, and half of

Chapter 3: Level of Awareness in the Private Healthcare Sector

the respondents would consider changing to another medical aid. The majority of the respondents always read their SOBAs, with specific focus on the total amount and the coverage from the medical aid in order to determine the amount they still owed. Some respondents have noticed a claim which they did not recognize, which they reported to the medical aid. If they were offered a free medical identity theft monitoring service, they would definitely consider using the service.

Part 5 focused on medical identity theft experience, revealing that a few respondents allowed family and non-family members to use their identity for medical care a few times, as they were unable to afford medical treatment or in the case of an emergency. A small percentage of the respondents identified their parents, children or other family members had been victims of medical identity theft for the purpose of healthcare service or treatment. The respondents learnt about the medical identity theft incident almost immediately to less than three months since receiving medical bills from the healthcare provider. The incidents were not reported immediately by some respondents, as the respondents were unsure who to inform and did not want to alarm the family. The incidents occurred as a result of a data breach or shared medical identity to another family member. Although some respondents indicated financial consequences occurred in regaining their identity, they either paid the debt, or the credit score dropped. Some respondents managed to resolve the incident whereas others are still in the process of resolving the medical identity theft incident in order to continue their medical aid membership and healthcare service without any disruption of service. The respondents' identity theft issue was usually resolved within one month, costing not more than R10 000 and they spent about five to 30 hours fixing the issues. In future, reviewing medical records and checking SOBAs will be the steps the respondents selected to follow to reduce the chance of being a medical identity theft victim.

Part 1 of the survey does not provide any learning specific to medical identity theft; therefore major themes (part 2 to part 5) which can be learnt are listed below:

- Respondents shows a very low awareness of medical identity theft.
- The respondents did not follow best practices as they did not know about medical identity theft.
- Respondents were not fully aware as to who should be informed of medical identity theft.
- Very few respondents experience medical identity theft in South Africa.

Chapter 3: Level of Awareness in the Private Healthcare Sector

The following section 3.9 gives the conclusion of Chapter 3.

3.9 Conclusion

Chapter 3 presented the levels of medical identity theft awareness of medical aid members in South Africa by referring to data gathered via a survey. Purposive sampling, volunteer sampling and snowball sampling techniques were used to collect survey responses within South Africa.

Chapter 4 reports on the drafting of best practices to be used as guidelines by medical aid members in South Africa to combat medical identity theft.

Chapter 4 **BEST PRACTICES TO ADDRESS MEDICAL IDENTITY THEFT AWARENESS**

4.1 Introduction

This chapter investigates best practices for addressing medical identity theft. Section 4.2 identifies a list of concerns associated with the themes identified in Chapter 3. The use of an inductive content analysis approach to perform a qualitative content analysis (QCA) is discussed in section 4.3. Twenty literature articles are identified through this process. A close analysis of these sources is detailed in section 4.4. Thereafter, existing best practices are analyzed and relationships between similar best practices are identified. This process is illustrated by Table 4.3 in section 4.5. The identification of categories based on meaningful phrases found within the list of best practices is discussed in section 4.6. The categories and best practices are reviewed to remove any redundant information, and the changes made are discussed in section 4.7. Finally, the continuous revision and refinement of the categories, with a focus on pre-emptive and retroactive measures, is discussed in section 4.8. This leads to the best practices for medical aid members, which are separated into pre-emptive and retroactive measures, being described and summarised in section 4.9. The relevance of these best practices to South Africa is discussed in section 4.10. The following sections will examine this study's research approach in greater detail.

4.2 Thematic Analysis of Concerns

A list of four high-level themes emerged from Chapter 3. This section further analyzes these themes and identifies a list of concerns associated with them.

Table 4.1: *Themes and Concerns Pertaining to Respondents*

Themes	List of Concerns
There was little awareness of medical identity theft among respondents.	<ul style="list-style-type: none"> • A lack of knowledge about medical identity theft • Inaccuracies in medical records
Respondents did not follow best practices, as they did not know about medical identity theft.	<ul style="list-style-type: none"> • Checking the accuracy of medical records • How medical records are checked (electronically or on paper)

Themes	List of Concerns
Respondents were not fully aware of who should be informed about medical identity theft.	<ul style="list-style-type: none"> • Not reviewing their SOB • Not knowing to whom an unrecognized claim should be reported
Very few respondents experienced medical identity theft in South Africa.	<ul style="list-style-type: none"> • The sharing of medical aid information • Not knowing to whom medical identity theft should be reported

The list of concerns identified in Table 4.1 will be analysed in section 4.10, which addresses the relevance of the best practices.

The following section will identify the approach used to investigate the best practices.

4.3 Approach

This research study will perform an inductive content analysis based on the qualitative data gathered from the literature. As illustrated in Figure 4.1, content analysis consists of three main phases, namely the preparation, organization, and report phases.

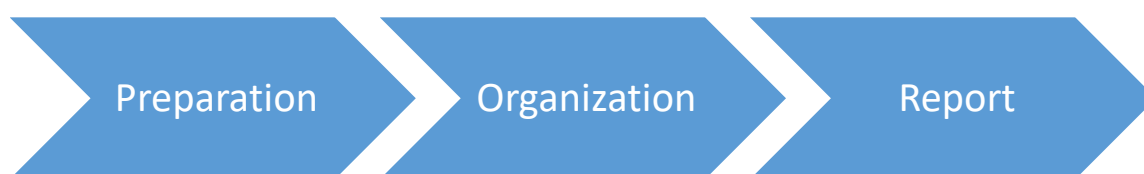


Figure 4.1: Phases of Content Analysis. Adapted from (Elo & Kyngäs, 2008)

Qualitative data is obtained from various literature sources. Sorting data into identifiable groups can improve the researcher’s understanding of the data and improve the quality and integrity of the research (Richards & Morse, 2013). A benefit of using multiple literature sources is that it minimizes any preconceived notions and improves the trustworthiness of the qualitative data gathered from the literature.

Elo et al. (2014) explain the phases of inductive content analysis, which are presented in Figure 4.1. **Preparation** involves the process of obtaining and analyzing data. **Organization** places data into categories to capture the information accurately. **Reporting** is based on the content analysis results and explains the phenomenon being studied using the selected approach.

Within this inductive QCA, preparation will entail reviewing the literature on best practices for addressing medical identity theft and identifying the best practices that are

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

aimed at medical aid members and not industries. Organization will entail comparing multiple literature sources and identifying similarities between the best practices found in various journals. A report will be created based on the results obtained from gathering and organizing the data to identify best practices for addressing medical identity theft.

The process of completing an inductive content analysis of qualitative data consists of the following steps (Thomas, 2013):

1. The preparation of raw data files
2. A close reading of the text
3. The creation of categories
4. Overlapping coding and uncoded text
5. The continuous revision and refinement of the category system

The following sections will elaborate on the steps of the inductive content analysis process.

4.4 Preparation of Raw Data Files

Thomas (2013) explains that the preparation of raw data files requires the researcher to “[f]ormat the raw data files in a common format (e.g., font size, margins, questions or interviewer comments highlighted)” (p. 241).

For this study, the inductive QCA process started with the identification of literature sources related to the objective of identifying best practices that can be used by medical aid members to address medical identity theft. From each literature source, a list of best practices was identified and stored in a spreadsheet. Table 4.2 identifies the 20 literature sources used within this inductive content analysis.

Table 4.2: *Literature Sources*

Organization	
1	American Dental Association (American Dental Association, 2014)
2	American Optometric Association (American Optometric Association, 2011)
3	Dental Abstracts (Dental Abstracts, 2019)
4	Australian Information Security Management Conference (Webb, 2007)

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

Organization	
5	Walden University (Clement, 2018)
6	The American Health Information Management Association (Eramo, 2016)
7	American Association of Retired Persons (AARP, 2019)
8	Federal Trade Commission Consumer Information (FTC, 2018)
9	The Balance (Siciliano, 2020)
10	Norton Life Lock (Norton Life Lock, 2019)
11	Forbes (Shin, 2015)
12	Norton Life Lock (Porter, 2002)
13	Consumer Report (Umansky, 2015)
14	World Privacy Forum (Dixon & Gellman, 2006)
15	The American Health Information Management Association (Rinehart-Thompson, 2008)
16	Debt (Debt, 2020)
17	United Texas Credit Union (United Texas Credit Union, 2016)
18	World Privacy Forum (WPF, 2007)
19	US Ponemon Institute (US Ponemon Institute, 2012)
20	US Ponemon Institute (US Ponemon Institute, 2015)

A variety of online publications and various academic databases, including ScienceDirect, EBSCOhost, Semantic Scholar, AHIMA, Google Scholar, and Google, were searched. Limited journal articles on topics related to best practice for medical aid members addressing medical identity theft were identified, therefore Google searches had to be used. The search strings used included “Medical identity theft”, “Best practice in medical identity theft”, “Prevent medical identity theft”, and “Safeguard medical

identity theft". The identified best practices come from a broad range of literature sources written from different perspectives, including academic journal articles and documents from financial organizations, consumers, the healthcare industry, and business and technology groups. A total of nine academic journal articles and 11 online publications from organizations were identified.

The following section will discuss a close reading of the text, focussing specifically on the best practices identified from the literature sources in Table 4.2.

4.5 Close Reading of Text

Thomas (2013) explains that "[o]nce text has been prepared, the raw text should be read in detail so the researcher is familiar with the content and gains an understanding of the 'themes' and details in the text" (p. 241).

In this section, a list of best practices is presented in order to gain an understanding of the themes within the literature sources. This list of best practices can be used as a guide by medical aid members dealing with medical identity theft. Many of the best practices identified from the 20 literature sources listed in Table 4.2 were nearly identical.

A step-by-step algorithm was used to collect the best practices listed in Table 4.3.

Step 1: Prepare the medical identity theft best practice literature article.

Step 2: Closely read the article and analyze the best practice.

Step 3: Check if the wording of the best practice is similar to that of a best practice in Table 4.3.

Step 4: If the wording of the best practice is not similar, go to Step 6.

Step 5: If the wording of the best practice is similar, go to Step 7.

Step 6: Add the wording of the best practice to Table 4.3 and place an "X" in the columns of the literature sources that connect to the best practice. Proceed to the next best practice. Go to Step 2.

Step 7: Place an "X" next to best practice that is similarly worded. Proceed to the next best practice. Go to Step 2.

These steps were used to check each best practice from each literature source to identify any similarities between the identified best practices. An "X" was placed in the

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

columns of the literature sources related to each best practice. The results of the execution of these steps are shown in Table 4.3.

Table 4.3: List of Best Practices

List of Best Practices		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	Safeguard your medical aid number and related information.	X			X						X		X			X	X		X	X	X
2	Do not give your medical aid information to family members or friends.	X						X												X	X
3	Shred all outdated medical documents. Keep electronic copies safe.	X						X	X		X		X				X			X	
4	Destroy prescription bottles before disposal.	X							X				X								
5	Do not jump on offers of free healthcare services or products.	X			X			X	X							X					
6	Before you share personal information on a	X							X				X								

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

List of Best Practices		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	website, find out why it is needed and how it will be stored. Read the privacy policy on the website.																				
7	Do not provide medical information over the phone or via email unless you initiated the call or email conversation.	X						X	X				X				X				
8	Get copies of your medical files from all your healthcare providers and review them to ensure their accuracy. (If you believe you are a victim, act quickly.)		X				X	X	X	X		X	X	X	X	X	X	X	X	X	X
9	Correct erroneous and false information in your files.		X		X		X		X	X			X		X		X	X		X	X

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

List of Best Practices		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
10	Request an accounting of disclosures.		X						X						X		X					
11	File a complaint if your privacy rights are violated. (For example, you may be refused copies of documents.)		X										X									
12	Educate data breach and financial identity theft victims about medical identity theft and the variations of the crime. (Protect private data.)			X	X														X			
13	Know that no provider will ever call you for information.			X													X	X				
14	Ask your medical aid (and all other providers) for a full list of the benefits paid out in your name annually.			X			X		X	X					X	X	X		X	X	X	
15	If your medical card is lost or				X						X						X					

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

List of Best Practices		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	stolen, report this to the appropriate provider immediately and ask for a replacement number.																				
16	File a police report. (Provide copies to your healthcare providers, medical aid, and credit reporting company.)				X	X	X							X	X						
17	Check your credit reports. (This can be done for free once a year.)				X	X	X			X	X	X	X	X	X		X		X	X	
18	Use a medical identity monitoring service.				X						X										
19	Get protective software (virus and malware protection).				X								X							X	
20	Use strong passwords for electronic devices.				X																

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

List of Best Practices		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	Review your SOB carefully and notify your medical aid of anything suspicious.						X	X		X	X	X	X		X		X	X		X	X
22	Do not provide medical information over the phone or via email to anyone who claims to be with a provider.							X													
23	Do not answer questions from callers who say they are conducting a survey and need your personal information (for example, your ID number).							X													
24	Safeguard digital and paper-based documents from all providers carefully (through encryption or by locking them in a safe).								X		X			X							X

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

List of Best Practices		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
25	If you share personal information online, look for the lock icon and “https” in the URL.								X				X								
26	File a report with the government.									X											
27	Share your ID number only when absolutely necessary.										X	X	X	X			X				
28	Learn to spot phishing emails.													X							
29	Choose between paper-based and digital documents. (Having both increases the chance of theft.)													X							
30	Never use public Wi-Fi.													X							
31	Be cautious when sharing medical information on the cloud.													X							
32	Be wary of wearables and the sharing of medical													X							

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

List of Best Practices		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	information on social media.																				
33	Share healthcare and financial information with trusted individuals only.															X				X	X
34	Contact your medical aid about charges for health care not provided.															X					
35	Engage with identity protection services. (Report concerns.)																X	X		X	X
36	Engage with your medical aid. (Report concerns or issues.)																X			X	X
37	Be wary of bills from third parties.																	X			
38	Distribute copies of discrepancies to all providers.																	X			
39	Raise awareness of the crime.																		X		X
40	Avoid internet transactions																			X	

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

List of Best Practices		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	involving confidential information.																				
41	Engage legal counsel to resolve incidents.																			X	X
42	Engage with healthcare providers. (Resolve concerns or issues.)																			X	X
43	Engage with the healthcare industry and healthcare professionals to resolve issues.																			X	X
44	Contact credit bureaus to fix errors in credit reports.																			X	X
45	Engage with non-profits that provide help and support.																				X

The best practices identified to enhance medical aid members' awareness of medical identity theft and thereby mitigate its consequences are listed in Table 4.3. The following section will discuss the creation of categories from the identified best practices.

4.6 Creation of Categories

Thomas (2013) explains the creation of categories as when “[t]he researcher identifies and defines categories or themes”. He further explains that “categories are created from meaning units or actual phrases used in specific text segments” (p. 241).

The best practices listed in Table 4.3 were analyzed, and categories were created based on the meaningful phrases identified. Furthermore, the category which best describes the nature of each best practice was identified. The following six categories emerged from this analysis:

1. Safeguard Healthcare Documents
2. Protect Medical Information
3. Electronic Check
4. Financial Check
5. Notify Officials
6. Awareness

The categorization of the 45 best practices is shown in Table 4.4.

Table 4.4: *List of Best Practices and Categories*

List of Best Practices and Categories		
1	Safeguard your medical aid number and related information.	Safeguard Healthcare Documents
2	Do not give your medical aid information to family members or friends.	Protect Medical Information
3	Shred all outdated medical documents. Keep electronic copies safe.	Safeguard Healthcare Documents
4	Destroy prescription bottles before disposal.	Protect Medical Information
5	Do not jump on offers of free healthcare services or products.	Protect Medical Information

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

List of Best Practices and Categories		
6	Before you share personal information on a website, find out why it is needed and how it will be stored. Read the privacy policy on the website.	Electronic Check
7	Do not provide medical information over the phone or via email unless you initiated the call or email conversation.	Protect Medical Information
8	Get copies of your medical files from all your healthcare providers and review them to ensure their accuracy. (If you believe you are a victim, act quickly.)	Safeguard Healthcare Documents
9	Correct erroneous and false information in your files.	Safeguard Healthcare Documents
10	Request an accounting of disclosures.	Financial Check
11	File a complaint if your privacy rights are violated. (For example, you may be refused copies of documents.)	Notify Officials
12	Educate data breach and financial identity theft victims about medical identity theft and the variations of the crime. (Protect private data.)	Awareness
13	Know that no provider will ever call you for information.	Protect Medical Information
14	Ask your medical aid (and all other providers) for a full list of the benefits paid out in your name annually.	Safeguard Healthcare Documents
15	If your medical card is lost or stolen, report this to the appropriate provider immediately and ask for a replacement number.	Protect Medical Information
16	File a police report. (Provide copies to your healthcare providers, medical aid, and credit reporting company.)	Notify Officials
17	Check your credit reports. (This can be done for free once a year.)	Financial Check

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

List of Best Practices and Categories		
18	Use a medical identity monitoring service.	Electronic Check
19	Get protective software (virus and malware protection).	Electronic Check
20	Use strong passwords for electronic devices.	Electronic Check
21	Review your SOB carefully and notify your medical aid of anything suspicious.	Safeguard Healthcare Documents
22	Do not provide medical information over the phone or via email to anyone who claims to be with a provider.	Protect Medical Information
23	Do not answer questions from callers who say they are conducting a survey and need your personal information (for example, your ID number).	Protect Medical Information
24	Safeguard digital and paper-based documents from all providers carefully (through encryption or by locking them in a safe).	Safeguard Healthcare Documents
25	If you share personal information online, look for the lock icon and “https” in the URL.	Electronic Check
26	File a report with the government.	Notify Officials
27	Share your ID number only when absolutely necessary.	Protect Medical Information
28	Learn to spot phishing emails.	Electronic Check
29	Choose between paper-based and digital documents. (Having both increases the chance of theft.)	Safeguard Healthcare Documents
30	Never use public Wi-Fi.	Electronic Check
31	Be cautious when sharing medical information on the cloud.	Electronic Check
32	Be wary of wearables and the sharing of medical information on social media.	Electronic Check

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

List of Best Practices and Categories		
33	Share healthcare and financial information with trusted individuals only.	Protect Medical Information
34	Contact your medical aid about charges for health care not provided.	Financial Check
35	Engage with identity protection services. (Report concerns.)	Notify Officials
36	Engage with your medical aid. (Report concerns or issues.)	Notify Officials
37	Be wary of bills from third parties.	Financial Check
38	Distribute copies of discrepancies to all providers.	Notify Officials
39	Raise awareness of the crime.	Awareness
40	Avoid internet transactions involving confidential information.	Electronic Check
41	Engage legal counsel to resolve incidents.	Notify Officials
42	Engage with healthcare providers. (Resolve concerns or issues.)	Notify Officials
43	Engage with the healthcare industry and healthcare professionals to resolve issues.	Notify Officials
44	Contact credit bureaus to fix errors in credit reports.	Notify Officials
45	Engage with non-profits that provide help and support.	Notify Officials

The 45 best practices were assigned to the six categories as follows:

- Safeguard Healthcare Documents – 8 best practices
- Protecting Medical Information – 10 best practices
- Electronic Check – 10 best practices
- Financial Check – 4 best practices
- Notify Officials – 11 best practices
- Awareness – 2 best practices.

The following section will examine overlapping coding and uncoded text in the context of best practices.

4.7 Overlapping Coding and Uncoded Text

Thomas (2013) explains that overlapping coding and uncoded text refers to two rules. The first rule is that “one segment of text may be coded into more than one category” (p. 242). The second rule is that “a considerable amount of the text may not be assigned to any category, as much of the text may not be relevant to the research objectives” (p. 242). For this study, identical best practices were identified to reduce redundant information. Furthermore, similar best practices were grouped into categories to ensure that a limited number of categories were created.

A step-by-step algorithm was used to identify redundant best practices. This process is illustrated in Tables 4.5 to 4.10.

Step 1: Create category tables using Table 4.4 (which is split up into Tables 4.5 to 4.10 according to the identified categories).

Step 2: Create acronyms for the categories based on the table headers (Example: SHD).

Step 3: Use the acronyms followed by sequence numbers to refer to the best practices (Example: SHD1).

Step 4: Compare each best practice in a category with every other best practice in the same category (Example: Compare SHD1 with SHD2 to SHD8).

Step 5: If a best practice shares similarities with other best practices in the same category, strike through the redundant ones (Example: ~~Know that no provider will ever call you for information~~). In the “Redundant” column, provide the acronym and sequence number of the best practice with a relationship to the best practices that were struck through (Example: PMI4). Go to Step 7.

Step 6: If a best practice shares no similarities with other best practices in the same category, go to Step 8.

Step 7: If best practices still exist within this category, proceed to the next best practice. Go to Step 4.

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

Step 8: Compare each best practice with every other best practice in the other categories. (Example: Compare SHD1 with PMI1 to PMI9, EC1 to EC11, etc. Exclude the removed best practices.)

Step 9: If a best practice shares similarities with other best practices in other categories, strike through the redundant ones (Example: ~~Know that no provider will ever call you for information~~). In the “Redundant” column, provide the acronym and sequence number of the best practice with a relationship to the best practices that were struck through (Example: PMI4). Go to Step 11.

Step 10: If a best practice shares no similarities with other best practices in other categories, go to Step 11.

Step 11: Proceed to the next best practice. Go to Step 8.

These steps were used to check whether the nature of a best practice was associated with more than one of the categories. After the best practices were assigned to tables, a redundancy check was performed to identify any similarities between the best practices. If similarities were found between best practices within the same category, the redundant best practices were removed and the remaining related best practice was identified using its acronym and a sequence number, for example SHD1. Once every best practice in a category had been checked, the remaining best practices were compared with the best practices from other categories. If similarities were found, the redundant best practices were removed.

No redundant best practices were found across categories. The only redundancies found existed within the categories.

This section contains the six categories identified in the previous section. The results of the execution of the described steps are presented in Tables 4.5 to 4.10. The first column of each of these tables contains the category acronyms and sequence numbers (for example, SHD1) of the best practices. The second column contains the best practices for medical identity theft awareness. The last column shows which best practices are related to the redundant best practices.

Table 4.5: *Safeguard Healthcare Documents*

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

Safeguard Healthcare Documents		Redundant
SHD1	Safeguard your medical aid number and related information.	
SHD2	Shred all outdated medical documents. Keep electronic copies safe.	
SHD3	Get copies of your medical files from all your healthcare providers and review them to ensure their accuracy. (If you believe you are a victim, act quickly.)	
SHD4	Correct erroneous and false information in your files.	
SHD5	Ask your medical aid (and all other providers) for a full list of the benefits paid out in your name annually.	
SHD6	Review your SOB carefully and notify your medical aid of anything suspicious.	
SHD7	Safeguard digital and paper-based documents from all providers carefully (through encryption or by locking them in a safe).	
SHD8	Choose between paper-based and digital documents. (Having both increases the chance of theft.)	

Table 4.6: *Protect Medical Information*

Protect Medical Information		Redundant
PMI1	Do not give your medical aid information to family members or friends.	
PMI2	Destroy prescription bottles before disposal.	
PMI3	Do not jump on offers of free healthcare services or products.	
PMI4	Do not provide medical information over the phone or via email unless you initiated the call or email conversation.	
PMI5	Know that no provider will ever call you for information.	PMI4

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

Protect Medical Information		Redundant
PMI6	If your medical card is lost or stolen, report this to the appropriate provider immediately and ask for a replacement number.	
PMI7	Do not provide medical information over the phone or via email to anyone who claims to be with a provider.	PMI4
PMI8	Do not answer questions from callers who say they are conducting a survey and need your personal information (for example, your ID number).	
PMI9	Share your ID number only when absolutely necessary.	PMI8
PMI10	Share healthcare and financial information with trusted individuals only.	

Table 4.7: *Electronic Check*

Electronic Check		Redundant
EC1	Before you share personal information on a website, find out why it is needed and how it will be stored.	
EC2	Use a medical identity monitoring service.	
EC3	Get protective software (virus and malware protection).	
EC4	Use strong passwords for electronic devices.	
EC5	If you share personal information online, look for the lock icon and “https” in the URL.	
EC6	Learn to spot phishing emails.	
EC7	Never use public Wi-Fi.	
EC8	Be cautious when sharing medical information on the cloud.	
EC9	Be wary of wearables and the sharing of medical information on social media.	

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

Electronic Check		Redundant
EC10	Avoid internet transactions involving confidential information.	EC1

Table 4.8: *Financial Check*

Financial Check		Redundant
FC1	Request an accounting of disclosures.	
FC2	Check your credit reports. (This can be done for free once a year.)	
FC3	Contact your medical aid about charges for health care not provided.	
FC4	Be wary of bills from third parties.	FC3

Table 4.9: *Notify Officials*

Notify Officials		Redundant
OC1	File a complaint if your privacy rights are violated. (For example, you may be refused of copies of documents.)	
OC2	File a police report. (Provide copies to your healthcare providers, medical aid, and credit reporting company.)	
OC3	File a report with the government.	OC1
OC4	Engage with identity protection services. (Report concerns.)	
OC5	Engage with your medical aid. (Report concerns or issues.)	
OC6	Distribute copies of discrepancies to all providers.	OC9
OC7	Engage legal counsel for help and support.	
OC8	Engage with non-profits that provide help and support.	OC7
OC9	Engage with healthcare providers. (Resolve concerns or issues.)	
OC10	Engage with the healthcare industry and healthcare professionals to resolve issues.	OC9
OC11	Contact credit bureaus to fix errors in credit reports.	

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

Table 4.10: Awareness

Awareness		Redundant
A1	Raise awareness of medical identity theft and the variations of the crime.	
A2	Raise awareness of the crime.	A1

This section closely analyzed each best practice within the six categories. Redundant best practices were removed to improve clarity. This reduction had the following effects on the categories:

- Safeguard Healthcare Documents – 8 best practices (no reduction of data)
- Protect Medical Information – 10 best practices reduced to 7
- Electronic Check – 10 best practices reduced to 9
- Financial Check – 4 best practices reduced to 3
- Notify Officials – 11 best practices reduced to 7
- Awareness – 2 best practices reduced to 1

The 45 best practices that were previously identified were reduced to 35 best practices.

The following section focuses on the continuous revision and refinement of the category system.

4.8 Continuous Revision and Refinement of Category System

Thomas (2013) explains that the continuous revision and refinement of the category system entails examining every category to “search for subtopics, including contradictory points of view and new insights” (p. 242).

Tables 4.5 to 4.10 show the reduction of the best practices within the categories. In this section, new insights lead to the revision and refinement of the best practice categories. Pre-emptive (before) and retroactive (after) best practices are distinguished from each other.

Pre-emptive best practices are measures that can be taken prior to an incident to minimize individuals’ chances of becoming victims of medical identity theft. Retroactive best practices are measures that can be taken after an incident, which can guide victims of medical identity theft in dealing with its repercussions. This section focuses on

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

identifying pre-emptive (Table 4.11) and retroactive (Table 4.12) best practices for addressing medical identity theft.

The best practices within the “Safeguard Healthcare Documents” table include not only safeguard measures, but also review measures. Thus, the “Safeguard Healthcare Documents” category was renamed the “Safeguard and Review Healthcare Documents” category to make it more explicit that the best practices in this category include review measures that can be used retroactively.

A step-by-step algorithm was used to identify the pre-emptive and retroactive best practices in Table 4.11 and Table 4.12.

Step 1: Analyze a best practice from the category.

Step 2: Determine the state (pre-emptive, retroactive, or both) of the best practice.

Step 3: If the best practice is a measure used prior to and after medical identity theft incidents, go to Step 6.

Step 4: If the best practice is a measure used prior to medical identity theft incidents, go to Step 7.

Step 5: If the best practice is a measure used after medical identity theft incidents, go to Step 8.

Step 6: Add the best practice to the pre-emptive table (Table 4.11) and the retroactive table (Table 4.12). Go to Step 9.

Step 7: Add the best practice to the pre-emptive table (Table 4.11). Go to Step 9.

Step 8: Add the best practice to the retroactive table (Table 4.12).

Step 9: Proceed to the next best practice in the category. Go to Step 1.

The results of the execution of the outlined steps are shown in Table 4.11 and Table 4.12. These steps were used to determine whether each best practice from each category is suitable for the pre-emptive table, the retroactive table, or both tables. The measures in Table 4.11 can be used by medical aid members prior to an incident of medical identity theft.

Table 4.11: *Pre-Emptive Best Practices*

Pre-Emptive Best Practices Addressing Medical Identity Theft	
Categories	Best Practices
Safeguard and Review Healthcare Documents	<ul style="list-style-type: none"> • Safeguard your medical aid number and related information. • Shred all outdated medical documents. Keep electronic copies safe. • Correct erroneous and false information in your files. • Ask your medical aid (and all other providers) for a full list of benefits paid out in your name annually. • Review your SOB carefully and notify your medical aid of anything suspicious. • Safeguard digital and paper-based documents from all providers carefully (through encryption or by locking them in a safe). • Choose between paper-based and digital documents. (Having both increases the chance of theft.)
Protect Medical Information	<ul style="list-style-type: none"> • Do not give your medical aid information to family members or friends. • Destroy prescription bottles before disposal. • Do not jump on offers of free healthcare services or products. • Do not provide medical information over the phone or via email unless you initiated the call or email conversation. • If your medical card is lost or stolen, report this to the appropriate provider immediately and ask for a replacement number. • Do not answer questions from callers who say they are conducting a survey and need your personal information (for example, your ID number). • Share healthcare and financial information with trusted individuals only.
Electronic Check	<ul style="list-style-type: none"> • Before you share personal information on a website, find out why it is needed and how it will be stored. • Use a medical identity monitoring service. • Get protective software (virus and malware protection). • Use strong passwords for electronic devices. • If you share personal information online, look for the lock icon and “https” in the URL.

Pre-Emptive Best Practices Addressing Medical Identity Theft	
Categories	Best Practices
	<ul style="list-style-type: none"> • Learn to spot phishing emails. • Never use public Wi-Fi. • Be cautious when sharing medical information on the cloud. • Be wary of wearables and the sharing of medical information on social media.
Financial Check	<ul style="list-style-type: none"> • Check your credit reports. (This can be done for free once a year.) • Contact your medical aid about charges for health care not provided.
Awareness	<ul style="list-style-type: none"> • Raise awareness of medical identity theft and the variations of the crime.

The identified list of pre-emptive best practices can be used to inform medical aid members about certain issues. For example, it can make them aware that they should request certain information from medical care providers to ensure that their medical records accurately reflect their doctor’s visits and prescriptions. Following these best practices can lessen the likelihood of becoming victims of medical identity theft.

Table 4.12: *Retroactive Best Practices*

Retroactive Best Practices Addressing Medical Identity Theft	
Categories	Best Practices
Safeguard and Review Healthcare Documents	<ul style="list-style-type: none"> • Get copies of your medical files from all your healthcare providers and review them to ensure their accuracy. (If you believe you are a victim, act quickly.)
Financial Check	<ul style="list-style-type: none"> • Request an accounting of disclosures.
Notify Officials	<ul style="list-style-type: none"> • File a complaint if your privacy rights are violated. (For example, you may be refused of copies of documents.) • File a police report. (Provide copies to your healthcare providers, medical aid, and credit reporting company.) • Engage with identity protection services. (Report concerns.)

Retroactive Best Practices Addressing Medical Identity Theft	
Categories	Best Practices
	<ul style="list-style-type: none"> • Engage with your medical aid. (Report concerns or issues.) • Engage legal counsel for help and support. • Engage with healthcare providers. (Resolve concerns or issues.) • Contact credit bureaus to fix errors in credit reports.

The retroactive best practices in Table 4.12 can be used as a guide by medical aid members who have become victims of medical identity theft. This will ensure that the medical aid members know how to proceed after becoming victims of medical identity theft.

No best practices were placed within both tables.

The best practices were divided between the pre-emptive and retroactive categories as follows:

- Pre-emptive best practices – 26
- Retroactive best practices – 9

The following section will expand on the identified best practices for medical identity theft.

4.9 Best Practices for Avoidance of Medical Identity Theft

The following sections briefly summarise each best practice. Section 4.9.1 focuses on pre-emptive measures, and section 4.9.2 focuses on retroactive measures.

4.9.1 Pre-emptive measures

In this subsection, five tables are used to represent five categories of best practices. Each table contains a column listing the best practices associated with the category and another column containing brief descriptions of these best practice.

Table 4.13: *Pre-Emptive Safeguard and Review Healthcare Documents Description and Summary*

Safeguard and Review Healthcare Documents		
Best Practice Description and Summary		
Safeguard your medical aid number and related information.	your aid and	<p>Protect your medical aid card number and insurance information by ensuring that they are stored securely (American Dental Association, 2014).</p> <p>Guard your medical aid card number and insurance information. Never leave documents containing healthcare information lying around out in the open.</p>
Shred all outdated medical documents. Keep electronic copies safe.		<p>Outdated paper-based medical documents from healthcare professionals and healthcare providers must be shredded before being disposed of, and digital copies must be secured (Federal Trade Commission Consumer Information, 2018).</p> <p>Outdated documents from doctors and other healthcare professionals should be disposed of properly to protect your medical information.</p>
Correct erroneous and false information in your files.	false	<p>If you notice any errors in your records, contact your doctors and your medical aid and inform them of the inaccurate information (American Optometric Association, 2011).</p> <p>Inform healthcare professionals and your medical aid if you notice any incorrect information in your medical files.</p>
Ask your medical aid (and all other providers) for a full list of the benefits paid out in your name annually.		<p>Once a year, a list of all the benefits paid out from your policy can be requested from your medical aid (Dental Abstracts, 2019).</p> <p>Request a list of the benefits paid out in your name from your medical aid yearly.</p>
Review your SOB carefully and notify your medical aid of	and your medical aid of	<p>Perform a comprehensive review of your SOB to ensure that all the treatments listed are medical treatments that you received (Siciliano, 2020).</p>

Safeguard and Review Healthcare Documents	
Best Practice Description and Summary	
anything suspicious.	Reviewing your SOB can determine whether all the medical treatments listed are familiar to you. If you notice that you never received a listed treatment, notify your medical aid.
Safeguard digital and paper-based documents from all providers carefully (through encryption or by locking them in a safe).	<p>Ensure that electronic records are properly encrypted and protected by security measures, such as passwords, and that paper-based records are locked in a secure place (Rotenstreich, n.d.).</p> <p>Protect any electronic medical documents using passwords and encryption and keep paper-based documents in a locked safe.</p>
Choose between paper-based and digital documents. (Having both increases the chance of theft.)	<p>Choose to keep either paper-based or digital records. Having both types of records can increase the chance of data theft (Umansky, 2015).</p> <p>To minimize the chance of records being lost, keep either digital or paper-based records of medical information. Having both types of records can increase the chance of loss or theft.</p>

Table 4.14: *Pre-Emptive Protect Medical Information Description and Summary*

Protect Medical Information	
Best Practice Description and Summary	
Do not give your medical aid information to family members or friends.	<p>Do not share your medical aid number or medical information with friends or family members in order for them to receive medical treatment using your identity (US Ponemon Institute, 2012).</p> <p>Do not give your medical aid information to family members or friends to use, as this can create inaccuracies in your medical records.</p>
Destroy prescription	Before disposing of prescription bottles with medical information on them, ensure that the labels are shredded or unreadable (Porter, 2002).

Protect Medical Information	
Best Practice Description and Summary	
bottles before disposal.	Dispose of prescription bottles carefully to ensure that no one else can use your medical information for their own purposes.
Do not jump on offers of free healthcare services or products.	Be careful if individuals offer you free healthcare services or products and request your medical aid number (Webb, 2007). Do not accept free healthcare services or treatments from individuals requesting any of your current medical aid information in person or telephonically.
Do not provide medical information over the phone or via email unless you initiated the call or email conversation.	Keep your medical information safe and secured and do not share it over the phone or via email (Debt, 2020). When receiving a phone call or an email, do not provide your medical information to an unknown individual unless you are aware of a reason to do so.
If your medical card is lost or stolen, report this to the appropriate provider immediately and ask for a replacement number.	If your medical aid card is lost or stolen, notify your medical aid and request a new card and number (Norton Life Lock, 2019). If your medical aid card is lost or stolen, contact your medical aid to replace the medical aid card and receive a new medical aid number. This will prevent anyone else from using your medical information in the future.
Do not answer questions from callers who say they are conducting a survey and need	Survey conductors are not required to collect personal information, such as your ID number, for research (American Association of Retired Persons, 2019).

Protect Medical Information	
Best Practice Description and Summary	
your personal information (for example, your ID number).	When asked to participate in a survey that requires personal information, such as your ID number, or confidential medical information, do not provide your personal or medical information.
Share healthcare and financial information with trusted individuals only.	<p>Share your medical information only with trusted individuals and organizations, such as healthcare professionals, the healthcare industry, and your medical aid (Rinehart-Thompson, 2008).</p> <p>When visiting a doctor, update them about any new information from other healthcare professionals. It is important to keep a record of new medical information and to have an accurate medical history.</p>

Table 4.15: *Pre-Emptive Electronic Check Description and Summary*

Electronic Check	
Best Practice Description and Summary	
Before you share personal information on a website, find out why it is needed and how it will be stored.	<p>Prior to sharing personal or medical information, such as your ID or medical aid number, online, check the privacy policy on the website to find out with whom your information will be shared and how the data will be stored (American Dental Association, 2014).</p> <p>When accessing a website that requires your personal medical information, view the privacy policy on the website to learn how the data will be stored.</p>
Use a medical identity monitoring service.	<p>Numerous companies worldwide have started offering identity theft protection, which uses proactive monitoring to notify individuals via email of any suspicious activities related to their medical information (Shin, 2015).</p> <p>The use of a medical identity monitoring service is necessary. However, such services are not yet available in South Africa. An alternative that can be used is a website called Identity Guard (Identity Guard, n.d.). Identity monitoring services alert you of any suspicious activities related</p>

Electronic Check	
Best Practice Description and Summary	
	to your personal information. These services can also assist in restoring your identity.
Get protective software (virus and malware protection).	<p>Malicious software can cause tremendous problems. Ensure that high-quality software is used to protect against viruses and malware and constantly update this software (Mirza, 2014).</p> <p>Always ensure that your computer has the latest virus and malware protection software. This will protect your device if hackers try to gain access to your medical and personal information.</p>
Use strong passwords for electronic devices.	<p>Use a strong password that is easy to remember but challenging for hackers to guess (Clement, 2018).</p> <p>Secure your laptop and cell phone with strong passwords to prevent hackers from gaining access to any data on your devices. Use a variety of uppercase and lowercase letters, numbers, and symbols to increase the difficulty of guessing your password.</p>
If you share personal information online, look for the lock icon and “https” in the URL.	<p>When sharing medical information online, look for a lock icon in the browser status bar and check whether the URL begins with “https” (Federal Trade Commission Consumer Information, 2018).</p> <p>When accessing or uploading personal medical information to medical sites, look for a lock icon and “https” in the URL, as these indicate a secure website.</p>
Learn to spot phishing emails.	<p>Do not open emails from unknown senders or click on links in such emails (Das, Kim, Tingle, & Nippert-Eng, 2019).</p> <p>If you receive an email from an email address you do not recognize, do not click on the email or any links in the email, as this could allow hackers to gain access to your ID number, passwords, and personal or medical documents.</p>

Electronic Check	
Best Practice Description and Summary	
Never use public Wi-Fi.	<p>Do not log in to your medical or financial accounts using public Wi-Fi, as this could allow hackers to gain access to your medical data (Umansky, 2015).</p> <p>Avoid using public Wi-Fi to access medical or financial information on mobile devices or laptops. Use a personal mobile network to access any websites containing medical information.</p>
Be cautious when sharing medical information on the cloud.	<p>Remember that not all cloud services offer equal levels of data protection. Use two-factor password authentication to protect medical data when uploading files to online storage accounts (Löhr, Sadeghi, & Winandy, 2010).</p> <p>When you log in to an online account using a username and password, you normally gain access immediately. When using two-factor authentication (an extra layer of security), you will have to provide another piece of information to gain access. This could be another password, biometric authentication, or the contents of an SMS sent to your registered cellular device.</p>
Be wary of wearables and the sharing of medical information on social media.	<p>Do not add your medical information to fitness device websites (for example, the Fitbit website) or share your personal track record on social media (Montgomery, Chester, & Kopp, 2018).</p> <p>When signing up for and configuring a fitness device account, avoid providing your medical information and sharing your fitness information on social media platforms (for example, Facebook).</p>

Table 4.16: *Pre-Emptive Financial Check Description and Summary*

Financial Check	
Best Practice Description and Summary	
Check your credit reports. (This can	An overview of your financial history can be requested for review from your credit bureau using your identity document (ID) (Siciliano, 2020).

Financial Check	
Best Practice Description and Summary	
be done for free once a year.)	Check your credit reports online on websites such as Experian. Provide your ID number to check your financial history for free once a year.
Contact your medical aid about charges for health care not provided.	<p>If you notice a charge for a service that was never received, contact your medical aid to raise concern and gain further insight (Rinehart-Thompson, 2008).</p> <p>If you notice an outstanding payment or a deduction from your medical aid account for a service that you did not receive, contact your medical aid and query the charge to your name.</p>

Table 4.17: Pre-Emptive Awareness Description and Summary

Awareness	
Best Practice Description and Summary	
Raise awareness of medical identity theft and the variations of the crime.	<p>Medical aid members need to be informed about medical identity theft and its consequences. They should also be taught how to keep their private medical data protected (World Privacy Forum, 2007).</p> <p>Generate a high level of awareness of medical identity theft and the dangers associated with it.</p>

Tables 4.13 to 4.17 provide brief descriptions of the pre-emptive best practices. These pre-emptive best practices belong to the following categories:

- Safeguard and Review Healthcare Documents – 7 best practices
- Protect Medical Information – 7 best practices
- Electronic Check – 9 best practices
- Financial Check – 2 best practices
- Awareness – 1 best practice

A total of 26 pre-emptive best practices that can be used by medical aid members to address medical identity theft were identified. The following section focuses on the retroactive best practices.

4.9.2 Retroactive measures

In this subsection, three tables are used to represent three categories of best practices. Each table contains a column listing the best practices associated with the category and another column containing brief descriptions of these best practices.

Table 4.18: *Retroactive Safeguard and Review Healthcare Documents Description and Summary*

Safeguard and Review Healthcare Documents	
Best Practice Description and Summary	
Get copies of your medical files from all your healthcare providers and review them to ensure their accuracy. (If you believe you are a victim, act quickly.)	Collect copies of medical files from healthcare professionals and healthcare providers to provide to officials as evidence (Porter, 2002) Request medical files from doctors and hospitals to use as evidence of discrepancies.

Table 4.19: *Retroactive Financial Check Description and Summary*

Financial Check	
Best Practice Description and Summary	
Request an accounting of disclosures.	An accounting of disclosures is a log report that keeps track of the release of a patient’s medical information to other individuals (American Optometric Association, 2011). Request an accounting of disclosures from healthcare providers or healthcare professionals if any of your protected health information (PHI) is released for reasons other than treatment, payment, or healthcare operations.

Table 4.20: *Retroactive Notify Officials Description and Summary*

Notify Officials	
Best Practice Description and Summary	
File a complaint if your privacy rights are violated. (For example, you may be refused copies of documents.)	<p>If a healthcare provider or medical aid refuses to provide a medical aid member with a copy of their medical records, the issue can be reported as a privacy rights violation (Amy-Vogt, 2020).</p> <p>If you request copies of your medical records from a healthcare provider or the healthcare industry and they rejected this request, go to the constitutional court to file a privacy rights violation complaint. You are entitled to copies of your personal medical records.</p>
File a police report. (Provide copies to your healthcare providers, medical aid, and credit reporting company.)	<p>File a report to inform the police of medical identity theft (Mancini, 2014).</p> <p>Report medical identity theft to the South African Police Service (SAPS) to obtain a case number.</p>
Engage with identity protection services. (Report concerns.)	<p>Once you have evidence that medical identity theft has occurred and your medical information has been stolen, notify your identity protection service of the issue (Walters & Betz, 2012).</p> <p>If you are an identity protection service member, report medical identity theft to the service.</p> <p>If you are not a member of any identity protection service, report medical identity theft to the South African Fraud Prevention Service (SAFPS), which offers free Protective Registration (PR), and register as victim of identity theft. Email or call the SAFPS to ask for an application form, which will have to be completed and returned along with a letter from the company where the impersonator used your identity. The SAFPS will process your application, issue a reference number, store your information in the SAFPS database, and inform all members associated with the SAFPS.</p>

Notify Officials	
Best Practice Description and Summary	
Engage with your medical aid. (Report concerns or issues.)	<p>If you notice any suspicious activities in your medical records, inform and provide the evidence to your medical aid provider (Experian, 2010).</p> <p>Inform your medical aid of any inaccuracies identified and wait for results, as these issues can take time to resolve. Rectifying these issues can be a long process, which may lead to further consequences that need to be dealt with.</p>
Engage legal counsel for help and support.	<p>Medical aid members who become victims of medical identity theft can seek legal advice and guidance from legal counsel. (US Ponemon Institute, 2012).</p> <p>Seek legal advice from a lawyer who can provide information on the laws regarding medical identity theft.</p>
Engage with healthcare providers. (Resolve concerns or issues.)	<p>Healthcare providers can be contacted to guide and assist medical aid members in rectifying problems caused by medical identity theft (US Ponemon Institute, 2015).</p> <p>If any problems such as medical identity theft occur, contact your healthcare providers to prevent further damage to your medical records.</p>
Contact credit bureaus to fix errors in credit reports.	<p>Inform credit bureaus of the theft of your medical identity to freeze any financial transactions (Federal Trade Commission Consumer Information, 2018).</p> <p>South Africa has 13 registered credit bureaus, such as Experian and TransUnion. Contact these credit bureaus, inform them that your medical identity has been stolen, and provide any copies of documents as evidence.</p>

Tables 4.18 to 4.20 provide brief descriptions of the retroactive best practices. These retroactive best practices belong to the following categories:

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

- Safeguard and Review Healthcare Documents – 1 best practice
- Financial Check – 1 best practice
- Notify Officials – 7 best practices

A total of nine retroactive best practices that can be used by medical aid members to address medical identity theft were identified. The following section examines the relevance of the best practices to South African medical aid members.

4.10 Relevance of the Best Practice to South African Medical Aid Members

In Chapter 3 (section 3.8), the contents of the questionnaire were summarised and themes were identified based on its sections. In Chapter 4 (section 4.2), the four high level themes were further analyzed and a list of concerns associated with these high level themes were identified.

This section examines the relevance of the best practices to South Africans. The best practices are mapped to the identified list of concerns in Table 4.21.

Table 4.21: *Relevance of Best Practices to South African Medical Aid Members*

List of Concerns	Relevant Best Practices
<ul style="list-style-type: none">• A lack of knowledge about medical identity theft	<ul style="list-style-type: none">• Raise awareness of medical identity theft and the variations of the crime.
<ul style="list-style-type: none">• Inaccuracies in medical records	<ul style="list-style-type: none">• Safeguard your medical aid number and related information.• Shred all outdated medical documents. Keep electronic copies safe.• Correct erroneous and false information in your files.
<ul style="list-style-type: none">• Checking the accuracy of medical records	<ul style="list-style-type: none">• Ask your medical aid (and all other providers) for a full list of the benefits paid out in your name annually.• Before you share personal information on a website, find out why it is needed and how it will be stored.• Get protective software (virus and malware protection).• Use strong passwords for electronic devices.

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

List of Concerns	Relevant Best Practices
	<ul style="list-style-type: none"> • If you share personal information online, look for the lock icon and “https” in the URL. • Learn to spot phishing emails. • Get copies of your medical files from all your healthcare providers and review them to ensure their accuracy. (If you believe you are a victim, act quickly.)
<ul style="list-style-type: none"> • How medical records are checked (electronically or on paper) 	<ul style="list-style-type: none"> • Safeguard digital and paper-based documents from all providers carefully (through encryption or by locking them in a safe). • Choose between paper-based and digital documents. (Having both increases the chance of theft.)
<ul style="list-style-type: none"> • Not reviewing their SOB 	<ul style="list-style-type: none"> • Review your SOB carefully and notify your medical aid of anything suspicious.
<ul style="list-style-type: none"> • Not knowing to whom an unrecognized claim should be reported 	<ul style="list-style-type: none"> • If your medical card is lost or stolen, report this to the appropriate provider immediately and ask for a replacement number. • Contact your medical aid about charges for health care not provided. • Check your credit reports. (This can be done for free once a year.)

List of Concerns	Relevant Best Practices
<ul style="list-style-type: none"> • The sharing of medical aid information 	<ul style="list-style-type: none"> • Do not give your medical aid information to family members or friends. • Do not provide medical information over the phone or via email unless you initiated the call or email conversation. • Do not answer questions from callers who say they are conducting a survey and need your personal information (for example, your ID number). • Sharing healthcare and financial information with trusted individuals only.
<ul style="list-style-type: none"> • Not knowing to whom medical identity theft should be reported 	<ul style="list-style-type: none"> • File a complaint if your privacy rights are violated. (For example, you may be refused copies of documents.) • File a police report. (Provide copies to your healthcare providers, medical aid, and credit reporting company.) • Engage with identity protection services. (Report concerns.) • Engage with your medical aid. (Report concerns or issues.) • Engage legal counsel for help and support. • Engage with healthcare providers. (Resolve concerns or issues.) • Contact credit bureaus to fix errors in credit reports.

Mapping the best practices to the list of concerns identified using the questionnaire determined whether all of the concerns were addressed.

In section 4.9, a total of 26 pre-emptive and nine retroactive best practices for medical aid members were identified as a result of the qualitative content analysis. The relevance of these best practices to the identified list of concerns was assessed. This resulted in 20 pre-emptive and eight retroactive best practices being selected to address the list of concerns, as shown in Table 4.21.

Chapter 4: Best Practices to Address Medical Identity Theft Awareness

This section identified the best practices related to the identified list of concerns. However, this does not mean that the other best practices should be excluded. All of the best practices from section 4.9 can still be relevant to medical aid members.

The following section concludes Chapter 4.

4.11 Conclusion

This dissertation established that the prevalence of medical identity theft is continuously increasing across the globe. Focus was placed on the impact of medical identity theft on medical aid members in South Africa. Consequences of medical identity theft include a financial burden being placed on the victims as well as inaccuracies in their medical records. Pre-emptive and retroactive best practices that medical aid members can use to address medical identity theft were identified. An inductive content analysis approach was used and a five-step plan was followed to analyze the gathered literature and identify best practices for medical aid members. The 35 best practices identified can be used as guidelines by medical aid members in South Africa to combat medical identity theft.

Chapter 5 **CONCLUSION**

5.1 Introduction

This final chapter provides a brief overview of each of the other chapters. Additionally, the problem statement, research questions, and research objectives are revisited. Furthermore, the validity of this research study is analysed, and the research contributions are discussed. Finally, the research limitations are identified, and future research opportunities are discussed.

5.2 Summary of Chapters

5.2.1 Chapter 1 – Introduction

Chapter 1 introduced medical identity theft as a type of identity theft within the healthcare sector and provided its background. The problem addressed by this dissertation was identified as the lack of awareness of medical identity theft among South African medical aid members. This problem statement led to the development of the primary and secondary research questions and objectives. The research methodology and research ethics were also briefly discussed.

5.2.2 Chapter 2 – Medical Identity Theft

In Chapter 2, the literature on healthcare sector role players was reviewed, and a diagrammatic representation of the healthcare sector was presented. The various types of databases maintained by the role players were also discussed. The topic of healthcare fraud was examined in detail. Focus was placed on medical identity theft, the parties causing it, and the parties affected by it. A case scenario was provided to interpret the effects of medical identity theft and provide clarity on its consequences.

5.2.3 Chapter 3 – Level of Awareness in the Private Healthcare Sector

In Chapter 3, the method of data collection was analysed and the questionnaire design was explained. This was followed by an explanation of the questionnaire distribution and the sampling of respondents. The survey questionnaire comprised five parts. In addition to demographic data, information was sought regarding healthcare provider privacy, medical aid privacy, and the medical identity theft experiences of the respondents. Finally, themes were extrapolated from the responses to the survey and a summary of these themes was provided.

5.2.4 Chapter 4 – Best practice to Address Medical Identity Theft Awareness

In this chapter, it was explained that a qualitative content analysis (QCA) approach was used to analyse the literature. This was followed by an explanation of the three steps of a QCA, namely preparing, organizing, and reporting. The information on medical identity theft best practices obtained from various literature sources was analysed in order to present a list of best practices that medical aid members in South Africa can use to protect their medical identities. Based on the themes identified in the previous chapter, a list of concerns was identified and the relevance of the best practices to South Africa was examined.

5.2.5 Chapter 5 Conclusion

The final chapter concludes the research by revisiting the research questions and objectives. Furthermore, the research contributions and limitations are discussed. Recommendations for future research are also provided.

5.3 Research Questions and Objectives

The problem statement for this research was originally defined in Chapter 1.

Table 5.1: *Problem Statement*

Problem Statement
The problem addressed by this research is the lack of awareness of medical identity theft among medical aid members.

In order to address the problem statement, research questions and objectives were formulated in Chapter 1. These research questions and the achievement of the research objectives will now be discussed.

Table 5.2: *Research Question 1 and Research Objective 1*

Research Question 1	Research Objective 1
Who are the parties causing and the parties affected by medical identity theft in the South African private healthcare sector?	Identify the parties causing and the parties affected by medical identity theft in the South African private healthcare sector.

Research Question 1	Research Objective 1
<p>Chapter 1 provided background information on medical identity theft, while Chapter 2 presented information on the role players involved in the healthcare sector. The private healthcare sector was then analysed. The roles of the role players in the healthcare sector were explained and further details were provided. A diagram identified the three role players involved in causing medical identity theft, namely hackers, perpetrators, and internal fraudsters. A summary of these role players' intentions was provided. The consequences of medical identity theft were discussed, and a diagrammatic representation of the healthcare sector as well as a case scenario was provided. A summary of the consequences of medical identity theft was also presented.</p>	

Table 5.3: *Research Question 2 and Research Objective 2*

Research Question 2	Research Objective 2
<p>What is the level of medical identity theft awareness among medical aid members in the South African private healthcare sector?</p>	<p>Determine the level of medical identity theft awareness among medical aid members in the South African private healthcare sector.</p>
<p>The literature review (Chapter 2) offered a brief understanding of medical identity theft. The survey questionnaire was briefly discussed in Chapter 1 and further explained in Chapter 3. The survey was targeted at South Africans who were or had been members of a medical aid. The questionnaire comprised a series of carefully constructed questions to be answered by the respondents. These questions were based on information from the US Ponemon Institute and aimed to identify the consequences of medical identity theft (for example, financial strain). A summary identified themes from each section of the survey questionnaire. These were used again in Chapter 4.</p>	

Table 5.4: *Research Question 3 and Research Objective 3*

Research Question 3	Research Objective 3
Which existing best practices can be used to address medical identity theft awareness?	Identify best practices to address medical identity theft awareness.
<p>Chapter 4 examined existing best practices identified through a review of a total of 20 literature sources. Furthermore, the research approach was discussed in detail. Themes that emerged in Chapter 3 were used to identify a list of concerns. Best practices derived from the information collected were organized and presented in a report. Finally, lists of pre-emptive and retroactive best practices for medical aid members in South Africa were created. The list of concerns identified in the beginning of Chapter 4 determined the relevance of the best practices to South Africa.</p>	

By achieving all the sub-objectives, the researcher was able to achieve the main research objective, which was to propose best practices that can be used to address medical aid members' awareness of medical identity theft in the South African private healthcare sector.

5.4 Validity

Validity refers to the trustworthiness of research, which is established by ensuring that the research results are faithful to the research objectives (Golafshani, 2003). In the past, it has been questioned whether qualitative research meets the criteria for the quality research (Leung, 2015). In Chapter 1 (section 1.5), it was mentioned that exploratory research is used to study new phenomena or to approach existing research topics from a different point of view. The use of a convergent parallel design was discussed in section 1.5, which detailed this study's research methods.

Therefore, the criteria for qualitative research are used to determine the validity of this research. Lincoln and Guba (2004) identify four criteria for trustworthiness in qualitative research, namely credibility, transferability, dependability, and confirmability. The achievement of these criteria by this dissertation will be discussed in the subsections 5.4.1 to 5.4.4.

5.4.1 Credibility

Credibility is defined as trustworthiness and is based on the accuracy of a researcher's work (Mills, Durepos, & Wiebe, 2010). The credibility of a study is enhanced by the research being thoroughly planned. The planning of this research study was discussed in Chapter 1 (section 1.5), which detailed the use of a mixed method design to answer the primary research question.

The adoption of well-established research methods supports the achievement of credibility in qualitative research (Shenton, 2004). The literature review, logical argumentation, survey, and qualitative content analysis methods used in this study are well-established methods in qualitative research. Additionally, the methods used were described in detail in this study.

5.4.2 Transferability

Transferability refers to whether qualitative results can be used in other study environments (Coghlan & Brydon-Miller, 2014b).

In this study, the survey completed by medical aid members aimed to determine South Africans' level of awareness of medical identity theft. The survey was dependent on the South African context; therefore, it was highly contextual. The cohort of South African participants provided survey results unique to the country of origin of the participants. The aim of the survey was not transferability.

The study findings related to the best practices to address medical identity theft can be used in contexts other than South Africa. This claim is made on the basis that the sources of the best practices were not specific to South Africa. Other researchers may find these best practices to be transferable to their own contexts. The context of this study was described in detail in Chapter 2 and Chapter 3, supporting the determination of transferability to other contexts.

5.4.3 Dependability

Dependability is indicated by the ability of another researcher to replicate a study and produce the same results (L. Given, 2008). In Chapter 1, section 1.5.1 and section 1.5.2 described the research process followed and the research methods used by this study in detail. Chapter 3 explained the study's methods of data collection (section 3.2) and data analysis (section 3.3), while Chapter 4 provided a step-by-step guide to performing

a qualitative content analysis. This will ensure that other researchers will be able to replicate this study and understand any differences in their research outputs.

5.4.4 Confirmability

Confirmability is achieved by ensuring that the researcher is unbiased when analysing the data. The research results should be representative of the participants' responses and not the researcher's interpretations (Forero et al., 2018). In order to achieve confirmability, the researcher has to ensure that the results are connected to the conclusion through the methods used and the process followed (Moon, Brewer, Januchowski-Hartley, Adams, & Blackman, 2016).

In this research study, the results of the survey used to determine the level of awareness of medical identity theft among South African medical aid members in the private healthcare sector were presented in Chapter 3 using descriptive statistics. These statistics were based on the inputs from the survey participants.

The compilation of the list of best practices for addressing medical identity theft (Chapter 4) required the researcher's interpretation to a large extent. A qualitative content analysis process was followed to ensure rigour. Additionally, the coding of the data was reviewed by the research supervisor, and a substantial number of best practices were analysed to assist in eliminating bias.

5.5 Research Contribution

As technology is progressing, South Africa is moving towards a digital environment. This leaves the healthcare sector facing the possibility of medical identity theft (Wakama, 2017). As previously mentioned in Chapter 1 (section 1.2), medical aid members in South Africa learn of medical identity theft only once they become victims thereof. No research on measures that South African medical aid members can take to protect themselves against medical identity theft is currently available.

Therefore, this research study makes two primary research contributions, namely a survey (Chapter 3) and a list of best practices that South Africans can adopt to address medical identity theft (Chapter 4).

A questionnaire previously used by the US Ponemon Institute was slightly modified to be suitable for South African medical aid members, as detailed in Chapter 3 (section 3.2.1). By applying a mixed method research design, this study was able to gather qualitative and quantitative data from respondents. The respondents who participated

Chapter 5: Conclusion

in the questionnaire survey indicated that the questionnaire had been insightful, as few of them had been aware of medical identity theft before the survey.

Several insights resulted from the data obtained from the respondents. Firstly, the respondents had a low level of awareness of medical identity theft. Secondly, they did not know which corrective actions should be taken after a medical identity theft incident. Thirdly, they were unsure about who needs to be informed about such incidents. Lastly, few respondents had experienced medical identity theft in the past. The questionnaire contributed towards identifying and learning about how respondents and their close family members experienced and dealt with medical identity theft.

Best practices were identified from various literature sources identifying ways in which medical aid members can address medical identity theft. In Chapter 3, themes were identified using the questionnaire data. In Chapter 4, a list of concerns pertaining to these themes was created. An inductive qualitative content analysis was performed using 20 literature sources identifying best practices (section 4.3). A sequence of steps were followed in order to compile the final lists of pre-emptive and retroactive best practices for medical aid members.

Twenty-six pre-emptive best practice measures that medical aid members can take prior to medical identity theft and nine retroactive best practice measures that medical aid members can take following medical identity theft were identified. It was shown that the identified best practices are relevant to the list of concerns raised in the South African context. Therefore, this study makes the contribution of a list of best practice measures that South African medical aid members can adopt to address medical identity theft.

The research presented within this dissertation has some limitations.

5.6 Limitations

The first limitation is related to the survey respondents. Only 143 respondents completed the survey, and more than 50% of the respondents were located in Gauteng. A goal of the survey was to obtain information from respondents throughout South Africa who had been a victim of or knew of someone who had been a victim of medical identity theft. This would allow the researcher to gain insight into the way these respondents approached medical identity theft issues. The use of snowball sampling assisted in reaching respondents throughout South Africa. However, the respondents who

Chapter 5: Conclusion

participated had limited knowledge of medical identity theft and the consequences thereof.

The second limitation concerns the identification of literature sources related to medical identity theft within South Africa (Chapter 2). The limited amount of literature available on medical identity theft in South Africa was problematic. Therefore, literature relating generally to the topic of medical identity theft had to be used. This emphasized that no research on this topic had been conducted in South Africa. Such research is needed to provide information about medical identity theft and best practices to South African medical aid members.

The third limitation of the study is found in bias due to the survey modality which favoured participation of younger respondents, who may not use medical services a lot. It was noted that nearly 55% of the total respondents were between the age of 18 and 35. Less than 5% of the population were over the age of 65, thus individuals who are more likely to use the medical aid, were minimally represented.

Therefore, the limited number of respondents who had been victims of medical identity theft, the lack of available sources of literature on medical identity theft in South Africa and survey modality presented research challenges.

5.7 Future Research

The available published research on medical identity theft in the South African private healthcare sector is limited. This presents an opportunity for further research into topics related to medical identity theft. The same research process can be used to target more respondents who currently are or have previously been medical aid members. Obtaining more respondents who can answer the questionnaire can provide deeper knowledge of South Africans' understanding of medical identity theft.

Possible topics for future research could include the practical use of the best practices identified in Chapter 4. The list of best practices could be provided to medical aid members by medical aid, and research information could be obtained from these members. Researchers could conduct further research on medical aid members' experiences with these best practices and develop a set of revised guidelines using the feedback received.

5.8 Final Word

The respondents who participated in the survey and provided their knowledge and experiences were key contributors to this research. The survey results showed that South Africans still lack knowledge of medical identity theft. It also confirmed that medical identity theft can have devastating consequences, including financial issues and inaccurate medical records.

The researcher hopes that this study has made a valuable contribution to the private healthcare sector by providing a list of best practices that can be used by medical aid members to address medical identity theft.

REFERENCE LIST

- US Ponemon Institute (2013). 2013 Survey on medical identity theft (February). Retrieved from http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf
- American Association of Retired Persons. (2019). Medical Identity Theft. Retrieved March 19, 2020, from <https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html>
- American Dental Association. (2014). Medical identity theft: How to protect yourself. *The Journal of the American Dental Association*, 145(3), 308. [https://doi.org/https://doi.org/10.1016/S0002-8177\(14\)60071-4](https://doi.org/https://doi.org/10.1016/S0002-8177(14)60071-4)
- American Optometric Association. (2011). Medical identity theft. *Journal of the American Optometric Association*, 82(5), 326–328. <https://doi.org/https://doi.org/10.1016/j.optm.2011.03.009>
- Amigorena, F. (2014). The threat from within: How to start taking internal security more seriously. *Computer Fraud and Security*, 2014(7), 5–7. [https://doi.org/10.1016/S1361-3723\(14\)70510-X](https://doi.org/10.1016/S1361-3723(14)70510-X)
- Amy-Vogt, B. (2020). As medical records are stolen and shared, data protection faces a crisis of faith. Retrieved May 11, 2020, from <https://siliconangle.com/2020/03/05/data-protection-faces-crisis-faith-medical-records-stolen-shared-thecube/>
- Andress, J., & Winterfeld, S. (2014). Black Hat Hacker - an overview. Retrieved February 1, 2020, from <https://www.sciencedirect.com/topics/computer-science/black-hat-hacker>
- Association of Certified Fraud Examiners. (2019). What is fraud? Retrieved February 2, 2020, from <https://www.acfe.com/fraud-101.aspx>
- Aveyard, H. (2010). *Doing a literature review in health and social care: A practical guide* (2nd Editio). Berkshire, Great Britain: Open University Press.
- Basu, S., Andrews, J., Kishore, S., Panjabi, R., & Stuckler, D. (2012). Comparative performance of private and public healthcare systems in low- and middle-income countries: A systematic review. *PLoS Medicine*, 9(6), 19. <https://doi.org/10.1371/journal.pmed.1001244>

- Bodhani, A. (2013). Warding off fraud [electronic medical records security]. *Engineering & Technology*, 8(10), 36–39. <https://doi.org/10.1049/et.2013.1001>
- Botsko, D. (2019). Healthcare Fraud 101. Retrieved October 15, 2019, from <https://legal.thomsonreuters.com/en/insights/articles/clear-investigation-software-healthcare-fraud-101>
- Brancato, G., Macchia, M., Murgia, M., Signore, M., Simeoni, G., Blanke, K., ... Hoffmeyer-Zlotnik, J. H. P. (2006). Handbook of Recommended Practices for Questionnaire Development and Testing in the European Statistical System. *European Commission Grant Agreement*, 142. Retrieved from http://ec.europa.eu/eurostat/documents/64157/4374310/13-Handbook-recommended-practices-questionnaire-development-and-testing-methods-2005.pdf/52bd85c2-2dc5-44ad-8f5d-0c6ccb2c55a0%0Ahttp://epp.eurostat.ec.europaipv6.eu/portal/page/portal/research_methodolo
- BusinessTech. (2019). The 5 biggest medical aid schemes in SA – what they offer, and how much they cost in 2019. Retrieved November 13, 2019, from <https://businesstech.co.za/news/finance/287446/the-5-biggest-medical-aid-schemes-in-sa-what-they-offer-and-how-much-they-cost-in-2019/>
- Carroll, L. (2019). Healthcare data hacking could lead to identity thefts. Retrieved November 22, 2019, from <https://www.reuters.com/article/us-health-privacy-cyber/healthcare-data-hacking-could-lead-to-identity-thefts-idUSKBN1W82K3>
- Cavoukian, A. (2008). Privacy in the clouds. *Identity in the Information Society*, 1(1), 89–108. <https://doi.org/10.1007/s12394-008-0005-z>
- CBS This Morning. (2019). *Hackers are stealing sensitive medical records and selling them on dark web*. CBS This Morning. Retrieved from <https://youtu.be/6kTDqStFS50>
- Cheung, A. K. L. (2014). Structured Questionnaires. In A. C. Michalos (Ed.), *Encyclopedia of Quality of Life and Well-Being Research* (pp. 6399–6402). Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-94-007-0753-5_2888
- Clement, V. (2018). Strategies to Prevent and Reduce Medical Identity Theft Resulting

in Medical Fraud. Retrieved April 6, 2020, from
<https://www.semanticscholar.org/paper/Strategies-to-Prevent-and-Reduce-Medical-Identity-Clement/f3e3f92c9a4c71db16796624c3ec5de809a62184#citing-papers>

Coghlan, D., & Brydon-Miller, M. (2014a). *Data Analysis. The SAGE Encyclopedia of Action Research*. Thousand Oaks, CA: SAGE Publications.
<https://doi.org/10.4135/9781446294406>

Coghlan, D., & Brydon-Miller, M. (2014b). Transferability. In *The SAGE Encyclopedia of Action Research* (pp. 1–6). Thousand Oaks, CA: SAGE Publications.
<https://doi.org/10.4135/9781446294406.n347>

Cohen, J. K. (2019). Hackensack Meridian pays hackers after ransomware attack. Retrieved February 4, 2020, from
<https://www.modernhealthcare.com/cybersecurity/hackensack-meridian-pays-hackers-after-ransomware-attack>

Congressional Budget Office. (2019). Common Terms in Health Information Technology. Retrieved November 19, 2019, from
<http://www.cbo.gov/sites/default/files/cbofiles/ftpdocs/91xx/doc9168/appendix.4.1.shtml>

Cornell Law School. (2017). Healthcare Fraud. Retrieved October 15, 2019, from
https://www.law.cornell.edu/wex/healthcare_fraud

Council for medical schemes. (2010). *Requirements for Medical Scheme Administrators*. Pretoria.

Creswell, J. W., & Plano Clark, V. L. (2010). *Designing and Conducting Mixed Methods Research - Google Books* (2nd ed.). California: SAGE Publications. Retrieved from
https://books.google.co.za/books/about/Designing_and_Conducting_Mixed_Methods_R.html?id=YcdIPWPJRBcC&printsec=frontcover&source=kp_read_button&redir_esc=y#v=onepage&q&f=true

D'Alfonso, S. (2015). The Growing Problem of Medical Identity Theft.
<https://doi.org/https://securityintelligence.com/the-growing-problem-of-medical-identity-theft/>

- Daniel, J. (2012). *Sampling essentials: Practical guidelines for making sampling choices*. Thousand Oaks, CA: SAGE Publications.
<https://doi.org/10.4135/9781452272047>
- Das, S., Kim, A., Tingle, Z., & Nippert-Eng, C. (2019). All About Phishing: Exploring User Research through a Systematic Literature Review. *ResearchGate*. Retrieved from <https://arxiv.org/ftp/arxiv/papers/1908/1908.05897.pdf>
- Davis. (2012). Growing health care fraud drastically affects all of us. Retrieved August 4, 2019, from <https://www.acfe.com/article.aspx?id=4294974475>
- Dean, P. C., Vazquez-Gonzalez, J., & Fricker, L. (2013). *Causes and Challenges of Healthcare Fraud in the US. International Journal of Business and Social Science* (Vol. 4). Florida. Retrieved from https://ijbssnet.com/journals/Vol_4_No_14_November_2013/1.pdf
- Debt. (2020). Medical Identity Theft: Stop Insurance Fraud. Retrieved March 19, 2020, from <https://www.debt.com/identity-theft/medical/>
- Dental Abstracts. (2019). Protecting against theft of your medical identity information. *Dental Abstracts*, 64(4), 222–223.
<https://doi.org/https://doi.org/10.1016/j.denabs.2019.03.014>
- Dietsche, E. (2018). Survey: 38% of hackers said they could find the healthcare data they sought in less than an hour. Retrieved February 4, 2020, from <https://medcitynews.com/2018/04/survey-38-of-hackers/?rf=1>
- Dixon, P. (2006). *MEDICAL IDENTITY THEFT: The Information Crime that Can Kill You. World privacy forum*. Los Angeles.
https://doi.org/http://www.worldprivacyforum.org/wp-content/uploads/2007/11/wpf_medicalidtheft2006.pdf
- Dixon, P., & Gellman, R. (2006). Consumer Tips: Medical Identity Theft- What to Do if You are a Victim (or are concerned about it). Retrieved March 19, 2020, from <https://www.worldprivacyforum.org/2012/04/consumer-tips-medical-id-theft-what-to-do-if-you-are-a-victim/>
- Dockterman, E. (2013). Your Identity Is Worth \$5 on the Black Market. Retrieved June 16, 2016, from <http://newsfeed.time.com/2013/08/26/your-identity-is-worth-5-on-the-black-market/>

- Drew, C. J., Hardman, M. L., & Hosp, J. L. (2007). The Research Process. *SAGE Publication*, 29–54. Retrieved from https://us.sagepub.com/sites/default/files/upm-binaries/26093_2.pdf
- Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative Content Analysis: A Focus on Trustworthiness. *SAGE*, 1–10. <https://doi.org/10.1177/2158244014522633>
- Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing*, 62(1), 107–115. <https://doi.org/10.1111/j.1365-2648.2007.04569.x>
- ENCA. (2018). Healthcare sector fraud on the rise. Retrieved October 15, 2019, from <https://www.enca.com/money/healthcare-sector-fraud-on-the-rise>
- Eramo, L. A. (2016). Stopping Thieves in Their Tracks: What HIM Professionals can do to Mitigate Medical Identity Theft. *Journal of AHIMA*, 87(8), 40–43. Retrieved from <https://bok.ahima.org/doc?oid=301836#.XopkrYgzbIV>
- Erasmus, S. (2016). Medical schemes - the basics. Retrieved August 21, 2020, from <https://www.health24.com/Medical-schemes/Choosing-a-medical-scheme/Medical-schemes-the-basics-20120721>
- Evans, R. S. (2016). Electronic Health Records: Then, Now, and in the Future. *Medical Informatics*, 48–61. <https://doi.org/10.15265/IYS-2016-s006>
- Expatica. (2019). A guide to the healthcare in South Africa. Retrieved October 15, 2019, from <https://www.expatica.com/za/healthcare/healthcare-basics/healthcare-in-south-africa-105896/>
- Experian. (2010). Combating the rising tide of medical identity theft. Retrieved May 11, 2020, from <https://www.experian.com/assets/data-breach/white-papers/medical-fraud-resolution.pdf>
- Federal Trade Commission Consumer Information. (2018). Medical Identity Theft. Retrieved March 19, 2020, from <https://www.consumer.ftc.gov/articles/0171-medical-identity-theft#protecting>
- Fedhealth. (2016). what is medical aid. Retrieved October 28, 2019, from <https://www.fedhealth.co.za/medical-aid-questions/what-is-medical-aid/>

- US Ponemon Institute (2015). Fifth annual study on medical identity theft (February). Retrieved from http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf
- Fitzgerald, R. J. (2009, June). Medication errors: The importance of an accurate drug history. *British Journal of Clinical Pharmacology*. US National Library of Medicine. <https://doi.org/10.1111/j.1365-2125.2009.03424.x>
- Forero, R., Nahidi, S., Costa, J. De, Mohsin, M., Fitzgerald, G., Gibson, N., ... Aboagye-Sarfo, P. (2018). Application of four-dimension criteria to assess rigour of qualitative research in emergency medicine. *BMC Health Services Research*, 18. <https://doi.org/10.1186/S12913-018-2915-2>
- Frankenfield, J. (2018). Medical Identity Theft. Retrieved August 27, 2019, from <https://www.investopedia.com/terms/m/medical-identity-theft.asp>
- Fraud in SA healthcare system. (2013). Retrieved from <https://www.health24.com/Medical-schemes/General-info/Fraud-in-SA-healthcare-system-20130319>
- Fraud Org. (1996). Medical ID theft. Retrieved February 4, 2020, from https://www.fraud.org/medical_id_theft
- Freitas, J. L., Bufrem, L. S., & Brenda, S. M. (2016). *Methodological choices for research in Information Science: Contributions to domain analysis1* (Vol. 28). Scielo. <https://doi.org/http://dx.doi.org/10.1590/2318-08892016002800001>
- Ga, O., Sa, F., & Med, F. F. (2014). Ethics in health care : healthcare fraud, 56(1), 10–13.
- Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: Interviews and focus groups. *British Dental Journal*, 204(6), 291–295. <https://doi.org/10.1038/bdj.2008.192>
- Gillespie, G. (2012, September). Disclosing patient records. *Medical Protection Society*, 28. https://doi.org/https://www.medicalprotection.org/docs/default-source/pdfs/casebook-pdfs/south-africa-casebook-pdfs/september-2012.pdf?sfvrsn=8c1170ac_2
- Given, L. (2008). *The SAGE Encyclopedia of Qualitative Research Methods*. The SAGE Encyclopedia of Qualitative Research Methods. Thousand Oaks, CA:

- SAGE Publications. <https://doi.org/10.4135/9781412963909>
- Given, L. M. (2011). *Descriptive Research*. (N. J. Salkind, Ed.). Thousand Oaks, CA: SAGE Publications. <https://doi.org/http://dx.doi.org/10.4135/9781412952644>
- Golafshani, N. (2003). *The qualitative report : An online journal dedicated to qualitative research. The Qualitative Report* (Vol. 8). Toronto: Nova Southeastern University, School of Social and Systematic Studies. Retrieved from <https://nsuworks.nova.edu/tqr/vol8/iss4/6>
- Goodwin, J., Woodfield, M., Ibnoaf, M., Koch, M., & Yan, H. (2006). Approach to data collection. *IPCC Guidelines for National Greenhouse Gas Inventories, 1*, 1–24. Retrieved from https://www.ipcc-nggip.iges.or.jp/public/2006gl/pdf/1_Volume1/V1_2_Ch2_DataCollection.pdf
- Grant, K. B., & Young, K. (2016). How to protect yourself from medical identity theft. Retrieved September 17, 2019, from <https://www.cnbc.com/2016/11/08/how-to-protect-yourself-from-medical-identity-theft.html>
- Gray, A., Riddin, J., & Jugathpal, J. (2016). Health Care and Pharmacy Practice in South Africa. *The Canadian Journal of Hospital Pharmacy*, 69(1), 36–41. <https://doi.org/10.4212/cjhp.v69i1.1521>
- Hedayati, A. (2012). An analysis of identity theft : Motives, related frauds, techniques and prevention. *Journal of Law and Conflict Resolution*, 4(January), 1–12. <https://doi.org/10.5897/JLCR11.044>
- Hsieh, H.-F., & Shannon, S. E. (2005). Three Approaches to Qualitative Content Analysis. *Nordic Journal of Digital Literacy*, 15(9), 1277–1288. <https://doi.org/10.1177/1049732305276687>
- Identity Guard. (n.d.). Identity Theft Protection South Africa - Identity Guard. Retrieved May 19, 2020, from <https://www.identityguard.co.za/>
- Johnson, T. P. (2014). Snowball Sampling: Introduction. In *Wiley StatsRef: Statistics Reference Online* (pp. 1–5). John Wiley & Sons. <https://doi.org/10.1002/9781118445112.stat05720>
- Jupp, V. (2018). *Volunteer Sampling*. (V. Jupp, Ed.). London, UK: SAGE Publications. <https://doi.org/http://dx.doi.org/10.4135/9780857020116>

- Katurura, M. C., & Cilliers, L. (2018). Electronic health record system in the public health care sector of South Africa: A systematic literature review. *African Journal of Primary Health Care & Family Medicine Affiliation*, 1(11), 8.
<https://doi.org/10.4102/phcfm.v10i1.1746>
- Key Health. (2019). Medical Aid Membership South Africa - Affordable Medical Aid. Retrieved October 28, 2019, from
<https://www.keyhealthmedical.co.za/members/scheme-info/news/339-medical-aid-membership-south-africa>
- Kolb, B. (2008). Determining Probability Samples In: Marketing Research. *SAGE Publications*, 177–193. <https://doi.org/10.4135/9780857028013>
- Kothari, C. R. (2004). *Research Methodology: Methods &; Techniques*. New Age International. Jaipur: NEW AGE INTERNATIONAL.
<https://doi.org/10.1017/CBO9781107415324.004>
- Kruse, C. S., Stein, A., Thomas, H., & Kaur, H. (2018, November 1). The use of Electronic Health Records to Support Population Health: A Systematic Review of the Literature. *Journal of Medical Systems*. Springer New York LLC.
<https://doi.org/10.1007/s10916-018-1075-6>
- Lavrakas, P. (2008). *Encyclopedia of Survey Research Methods*. Thousand Oaks, CA: SAGE Publications. <https://doi.org/10.4135/9781412963947>
- Lavrakas, P. J. (2018). Closed-Ended Question. *SAGE Publication*.
<https://doi.org/http://dx.doi.org/10.4135/9781412963947>
- Ledesma, A., Mcculloh, C., Wieck, H., & Yang, M. (2019). *Health Care Sector Overview*. Washington. Retrieved from
https://s3.wp.wsu.edu/uploads/sites/606/2015/02/SectorOverview_HC_Spring2014.pdf
- Legotlo, T. G., Hons, B., Mutezo, A., & Hons, B. (2018). Understanding the types of fraud in claims to South African medical schemes, *108*(4), 299–303.
<https://doi.org/10.7196/SAMJ.2018.v108i4.12758>
- Lester, M., Boateng, S., Studeny, J., & Coustasse, A. (2016). Personal Health Records: Beneficial or Burdensome for Patients and Healthcare Providers? *Perspectives in Health Information Management*, 13. Retrieved from

<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4832132/>

- Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, 4(3), 324–327. <https://doi.org/10.4103/2249-4863.161306>
- Lewis-Beck, M., Bryman, A., & Futing Liao, T. (2004). *The SAGE Encyclopedia of Social Science Research Methods*. Sage Publication. <https://doi.org/10.4135/9781412950589>
- Li, J., Huang, K.-Y., Jin, J., & Shi, J. (2008). A survey on statistical methods for health care fraud detection. *Health Care Management Science*, 11(3), 275–287. <https://doi.org/10.1007/s10729-007-9045-4>
- Lincoln, Y. S., & Guba, E. G. (2004). But is it rigorous? Trustworthiness and authenticity in naturalistic evaluation. *New Directions for Program Evaluation*, 1986(30), 73–84. <https://doi.org/10.1002/ev.1427>
- Liou, F., Tang, Y., & Chen, J. (2008). Detecting hospital fraud and claim abuse through diabetic outpatient services, 353–358. <https://doi.org/10.1007/s10729-008-9054-y>
- Löhr, H., Sadeghi, A. R., & Winandy, M. (2010). Securing the e-health cloud. In *IHI'10 - Proceedings of the 1st ACM International Health Informatics Symposium* (pp. 220–229). Arlington: ResearchGate. <https://doi.org/10.1145/1882992.1883024>
- Loxton, D. (2017). 200% spike in identity theft cause for concern. Retrieved June 17, 2018, from <https://www.iol.co.za/capetimes/news/200-spike-in-identity-theft-cause-for-concern-8103311>
- Luizzo, A., & Scaglione, B. (2014). Aspects of controlling fraud in healthcare facilities: taking the threat seriously. *Journal of Healthcare Protection Management*, 28(1), 21–27. Retrieved from <https://www.ncbi.nlm.nih.gov/pubmed/22423517>
- Mancini, M. (2014). Medical Identity Theft in the Emergency Department: Awareness is Crucial. *Western Journal of Emergency Medicine*, 15(7), 899–901. <https://doi.org/10.5811/westjem.2014.8.22438>
- Manerikar, V., & Manerikar, S. (2014). *A Note on Exploratory Research*. RESEARCH COMMUNICATION (Vol. XVII). Mumbai, India: Welingkar. Retrieved from <https://www.semanticscholar.org/paper/A-Note-on-Exploratory-Research->

Manerikar-Manerikar/c43ea45e4e940c8cb82758205c53b29b3e431c68

- Mills, A., Durepos, G., & Wiebe, E. (2010). *Encyclopedia of Case Study Research*. Thousand Oaks, CA: SAGE Publications. <https://doi.org/10.4135/9781412957397>
- Mirza, M. (2014). Malicious Software Detection, Protection & Recovery Methods a Survey. Retrieved May 10, 2020, from https://www.researchgate.net/publication/272997042_MALICIOUS_SOFTWARE_DETECTION_PROTECTION_RECOVERY_METHODS_A_SURVEY
- Mohan, A. (2014). A Medical Domain Collaborative Anomaly Detection Framework for Identifying Medical Identity Theft. In *2014 International Conference on Collaboration Technologies and Systems* (pp. 428–435). IEEE Computer Society. <https://doi.org/10.1109/CTS.2014.6867600>
- Molefe, P. (2018). *Fraud in the medical schemes industry*. Centurion. Retrieved from <https://www.masthead.co.za/wp-content/uploads/2018/06/CMSNews1of2018.pdf>
- MoneyMarketing. (2017). Medical aid fraud is a criminal offence. Retrieved August 28, 2019, from <https://www.moneymarketing.co.za/fighting-fraud-in-the-healthcare-industry/>
- Montgomery, K., Chester, J., & Kopp, K. (2018). Health Wearables: Ensuring Fairness, Preventing Discrimination, and Promoting Equity in an Emerging Internet-of-Things Environment. *Information Policy*, 8, 34–77. <https://doi.org/10.5325/jinfopoli.8.2018.0034>
- Moon, K., Brewer, T. D., Januchowski-Hartley, S. R., Adams, V. M., & Blackman, D. A. (2016). A guideline to improve qualitative social science publishing in ecology and conservation journals. *Ecology and Society*, 21(3), 17. <https://doi.org/10.5751/ES-08663-210317>
- National Health Care Anti-Fraud Association. (2018). Consumer Info. Retrieved October 15, 2019, from <https://www.nhcaa.org/resources/health-care-anti-fraud-resources/consumer-info-action.aspx>
- Norton Life Lock. (2019). What is Medical Identity Theft. Retrieved April 6, 2020, from <https://www.lifelock.com/learn-identity-theft-resources-what-is-medical-identity-theft.html>
- Ogunbanjo, G. A., & Makgatho, S. (2016). Ethics in health care : Healthcare fraud

Ethics in health care : healthcare fraud, (November).

Olivier, M. S. (2009). *Information Technology Research : A practical guide for Computer Science and Informatics*. Retrieved May 5, 2020, from <https://www.vanschaik.com/ebook/5121f4fb16757/>

Orton-Jones, C. (2017). *Getting into the mind of a fraudster*. Retrieved February 1, 2020, from <https://www.raconteur.net/risk-management/getting-into-the-mind-of-a-fraudster>

Patton, M. Q. (2014). *Qualitative Research & Evaluation Methods: Integrating Theory and Practice* - Michael Quinn Patton - Google Books. Retrieved June 26, 2020, from https://books.google.co.za/books?hl=en&lr=&id=ovAkBQAAQBAJ&oi=fnd&pg=PP1&ots=ZQ3X2vyDD-&sig=b59FvVQjP11IUHSVC3wZ86h_Bd4&redir_esc=y#v=onepage&q=2002&f=false

Phua, C., Lee, V., Smith, K., & Gayler, R. (1998). *A Comprehensive Survey of Data Mining-based Fraud Detection Research*. Melbourne. Retrieved from <https://arxiv.org/ftp/arxiv/papers/1009/1009.6119.pdf>

Porter, K. (2002). *3 Ways to Help Protect Against Medical ID Theft*. Retrieved March 19, 2020, from <https://www.lifelock.com/learn-identity-theft-resources-how-to-prevent-medical-identity-theft.html>

Richards, L., & Morse, J. M. (2013). *Readme first for a user's guide to qualitative methods*. SAGE Publications. Retrieved from https://books.google.co.za/books?hl=en&lr=&id=BKMKc7_Vac0C&oi=fnd&pg=PP1&dq=Read+me+first+for+a+users+guide+to+qualitative+methods&ots=gECrgl9Pkm&sig=VeUpZ9po5Aq5gptxrr_9LQ938mk&redir_esc=y#v=onepage&q=qualitative&f=false

Rinehart-Thompson, L. A. (2008). *Raising Awareness of Medical Identity Theft: For Consumers, Prevention Starts with Guarding, Monitoring Health Information*. *Journal of AHIMA*, 79(10), 74–75;81. Retrieved from <http://library.ahima.org/doc?oid=85512#.XnPTMIgzaUI>

Rotenstreich, S. (n.d.). *The Difference between Electronic and Paper Documents*.

- George Washington University. Retrieved from <https://www2.seas.gwu.edu/~shmuel/WORK/Differences/Chapter 3 - Sources.pdf>
- Rouse, M. (2017). electronic health record (EHR). Retrieved November 13, 2019, from <https://searchhealthit.techtarget.com/definition/electronic-health-record-EHR>
- Rouse, M. (2019). What is hacker? Retrieved February 1, 2020, from <https://searchsecurity.techtarget.com/definition/hacker>
- Rowe, K., & Moodley, K. (2013). Patients as consumers of health care in South Africa: The ethical and legal implications. *BMC Medical Ethics*, 14(1), 9. <https://doi.org/10.1186/1472-6939-14-15>
- Schaffer, P. (2018). Data Breaches on the Rise: How Healthcare Organizations Can Protect Against Medical Identity Theft. Retrieved September 26, 2019, from <https://www.idigitalhealth.com/news/data-breaches-on-the-rise-how-healthcare-organizations-can-protect-against-medical-identity-theft>
- Security News. (2016). Healthcare under Attack: What Happens to Stolen Medical Records? Retrieved October 20, 2019, from <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/healthcare-under-attack-stolen-medical-records>
- Sedgwick, P. (2014). Convenience Sampling. In *Encyclopedia of Measurement and Statistics*. SAGE Publications. <https://doi.org/10.4135/9781412952644.n107>
- Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, 22(2), 63–75. <https://doi.org/10.3233/EFI-2004-22201>
- Shin, L. (2015). Why Medical Identity Theft Is Rising And How To Protect Yourself. Retrieved September 14, 2019, from <https://www.forbes.com/sites/laurashin/2015/05/29/why-medical-identity-theft-is-rising-and-how-to-protect-yourself/#6158367c3608>
- Siciliano, R. (2020). Common Types of Medical Identity Theft. Retrieved March 20, 2020, from <https://www.thebalance.com/common-types-of-medical-identity-theft-4157717>
- Skela-Savič, B., MacRae, R., Lillo-Crespo, M., & Rooney, K. D. (2017). The Development of A Consensus Definition for Healthcare Improvement Science

- (HIS) in Seven European Countries: A consensus methods approach. *Zdravstveno Varstvo*, 56(2), 82–90. <https://doi.org/10.1515/sjph-2017-0011>
- Stateline, M. O. (2014). The Rise Of Medical Identity Theft In Healthcare | Kaiser Health News. Retrieved August 25, 2019, from <https://khn.org/news/rise-of-identity-theft/>
- Stocks, G. (2016). South African medical scheme administrators need to work together to benefit members. Retrieved October 23, 2019, from <https://bsg.co.za/2016/11/south-african-medical-scheme-administrators-need-to-work-together-to-benefit-members/>
- Stowell, N. F., Schmidt, M., & Wadlinger, N. (2018, October 1). Healthcare fraud under the microscope: improving its prevention. *Journal of Financial Crime*. Emerald. <https://doi.org/10.1108/JFC-05-2017-0041>
- Taherdoost, H. (2016). Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. *SSRN Electronic Journal*, 5(2), 18–27. <https://doi.org/10.2139/ssrn.3205035>
- Ponemon Institution (2012). Third annual survey on medical identity theft (June). Retrieved from www.ponemon.org/local/upload/file/Third_Annual_Survey_on_Medical_Identity_Theft_FINAL.pdf
- Thomas, D. R. (2013). A general inductive approach for qualitative data analysis. *School of Population Health*, 237–246. Retrieved from http://www.frankumstein.com/PDF/Psychology/Inductive_Content_Analysis.pdf
- Thornton, D., Brinkhuis, M., Amrit, C., & Aly, R. (2015). Categorizing and Describing the Types of Fraud in Healthcare. *Procedia - Procedia Computer Science*, 64, 713–720. <https://doi.org/10.1016/j.procs.2015.08.594>
- Umansky, D. (2015). 10 Ways To Protect Yourself From Medical Identity Theft. Retrieved March 19, 2020, from <https://www.consumerreports.org/cro/news/2015/05/10-ways-to-protect-yourself-from-medical-identity-theft/index.htm>
- United Texas Credit Union. (2016). Medical Identity Theft. Retrieved March 19, 2020, from <https://utxcu.com/blog/medical-identity-theft/>

- University of Miami Miller School of Medicine. (2019). Identity theft: Medical Identity Theft. Retrieved August 25, 2019, from <http://privacy.med.miami.edu/identity-theft/medical-identity-theft>
- Wakama, A. (2017). SA healthcare braces to take on risk. Retrieved July 19, 2020, from <https://www.itnewsafrika.com/2017/02/sa-healthcare-braces-to-take-on-risk/>
- Walliman, N. (2010). *Research Methods : The Basics*. Routledge. New York: Taylor & Francis e-Library. <https://doi.org/doi:10.4324/9780203836071>
- Walters, W., & Betz, A. (2012). Faculty Research & Creative Activity. *Medical Identity Theft*, 29, 75–79. Retrieved from http://thekeep.eiu.edu/fcs_fac/16
- Wang, J., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *Management Information Systems Quarterly*, 39(1), 91–112. Retrieved from <http://misq.org/misq/downloads>
- Webb, D. (2007). Medical Identity Theft – Not Feeling Like Yourself? In *Australian Information Security Management Conference* (pp. 216–225). Perth Western Australia: Edith Cowan University. <https://doi.org/10.4225/75/57b5548bb8765>
- Werner, A. (2019). Hackers are stealing millions of medical records – and selling them on the dark web. Retrieved August 19, 2019, from <https://www.cbsnews.com/news/hackers-steal-medical-records-sell-them-on-dark-web/>
- White, M. D., & Fisher, C. (2008). Assessing Our Knowledge of Identity Theft The Challenges to Effective Prevention and Control Efforts. *Criminal Justice*, (2003), 3–24. Retrieved from https://www.researchgate.net/publication/249720322_Assessing_Our_Knowledge_of_Identity_TheftThe_Challenges_to_Effective_Prevention_and_Control_Efforts
- William, M. K. (2006). Descriptive Statistics. Retrieved August 7, 2018, from <https://www.socialresearchmethods.net/kb/statdesc.htm>
- World Privacy Forum. (2007). Briefing Paper – Responses to Medical Identity Theft: Eight best practices for helping victims of medical identity theft. Retrieved March 19, 2020, from <https://www.worldprivacyforum.org/2007/10/medicalidtheftresponses/>

Yang, K. (2010). The Logic of Sampling. In *Making Sense of Statistical Methods in Social Research* (pp. 34–50). London, UK: SAGE Publications.
<https://doi.org/10.4135/9781473914636.n4>

APPENDIX A – ETHICS APPROVAL



PO Box 77000, Nelson Mandela University, Port Elizabeth, 6031, South Africa mandela.ac.za

Chairperson: Faculty of EBEIT Research Ethics Committee (Human)
Tel: +27 (0)41 504 3142
bertram.haskins@mandela.ac.za

NHREC registration nr: REC-042508-025

Ref: [H19-ENG-ITE-005] / Approval]

31 October 2019

PROF D POTTAS
Faculty: EBEIT

Dear PROF D POTTAS

GUIDELINES TO ADDRESS MEDICAL IDENTITY THEFT AWARENESS: THE CASE OF SOUTH AFRICAN MEDICAL AID MEMBERS

PRP: PROF D POTTAS
PI: MR B AH WHY

Your above-entitled application served at the Faculty of Engineering, the Built Environment and IT Research Ethics Committee (Human) (meeting of 29 OCTOBER 2019) for approval. The study is classified as a LOW risk study. The ethics clearance reference number is **H19-ENG-ITE-005** and approval is subject to the following conditions:

1. The immediate completion and return of the attached acknowledgement to Imtiaz.Khan@mandela.ac.za, the date of receipt of such returned acknowledgement determining the final date of approval for the study where after data collection may commence.
2. Approval for data collection is for 1 calendar year from date of receipt of above mentioned acknowledgement.
3. The submission of an annual progress report by the PRP on the data collection activities of the study (form RECH-004 to be made available shortly on Research Ethics Committee (Human) portal) by 15 November this year for studies approved/extended in the period October of the previous year up to and including September of this year, or 15 November next year for studies approved/extended after September this year.
4. In the event of a requirement to extend the period of data collection (i.e. for a period in excess of 1 calendar year from date of approval), completion of an extension request is required (form RECH-005 to be made available shortly on Research Ethics Committee (Human) portal)
5. In the event of any changes made to the study (excluding extension of the study), completion of an amendments form is required (form RECH-006 to be made available shortly on Research Ethics Committee (Human) portal).
6. Immediate submission (and possible discontinuation of the study in the case of serious events) of the relevant report to RECH (form RECH-007 to be made available shortly on Research Ethics Committee (Human) portal) in the event of any unanticipated problems, serious incidents or adverse events observed during the course of the study.
7. Immediate submission of a Study Termination Report to RECH (form RECH-008 to be made available shortly on Research Ethics Committee (Human) portal) upon unexpected closure/termination of study.
8. Immediate submission of a Study Exception Report of RECH (form RECH-009 to be made available shortly on Research Ethics Committee (Human) portal) in the event of any study deviations, violations and/or exceptions.
9. Acknowledgement that the study could be subjected to passive and/or active monitoring without prior notice at the discretion of the Research Ethics Committee (Human).

Please quote the ethics clearance reference number in all correspondence and enquiries related to the study. For speedy processing of email queries (to be directed to Imtiaz.Khan@mandela.ac.za), it is recommended that the ethics clearance reference number together with an indication of the query appear in the subject line of the email.

We wish you well with the study.

Yours sincerely

Dr B Haskins

Chairperson: Faculty of EBEIT Research Ethics Committee (Human)

Cc: Department of Research Capacity Development
Faculty Officer: EBEIT

Appendix 1: Acknowledgement of conditions for ethical approval

APPENDIX B – INFORMED CONSENT

Informed Content

Dear Participant,

You are invited to participate in a survey that aims to **determine the level of medical identity theft awareness among South African medical aid members in the private healthcare sector.**

The questions pertain to your knowledge of and possible experience with medical identity theft.

Medical identity theft is where someone uses a patient's personal identity information to obtain medical treatment, services or goods, including attempts to commit fake billing.

A Statement of Benefit (SOB) is a document or letter that is sent to you by your medical aid after you used a healthcare service that was claimed for through your medical aid company. You should get a SOB if you are a member of a medical aid.

You must be over the age of 18 to participate in this research.

You must be currently or previously a member of medical aid.

It will take approximately 10 minutes to complete the questionnaire.

Please note that:

- Your participation is completely voluntary. You have the right to withdraw from the study at any stage.
- There are no foreseeable risks associated with this project.
- Your survey responses will be strictly anonymous and confidential. This information as well as the results of the survey will remain strictly confidential.
- Data from this research will be reported only in the aggregate. Your information will be coded and will remain confidential and will only be viewed by myself and my research supervisor.

- The information from this questionnaire may be used for conference presentations and publication in academic journals.
- There will be no monetary benefits as a result of participating in the study

Thank you for taking time to consider participating in this study. If you have questions at any time about the questionnaire, you are more than welcome to contact Brandon Ah Why by email at s217405231@mandela.ac.za. Thank you very much for your time and support.

- I Agree “Checkbox” indicates:
 - Your consent to participate;
 - That you are 18 years or older; and
 - I am currently or previously been a member of medical aid.

I Agree

Submit