

---

*The Department of Software Engineering  
The University of Auckland  
New Zealand*

---

**Perceptions of HIPAA Security  
Requirements by US Dental  
Schools**

---

*Jinho Lee  
September 2006*

*Supervisors:*

*Professor Clark Thomborson*



A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE  
REQUIREMENTS OF MASTER OF ENGINEERING

# The University of Auckland

## Thesis Consent Form

This thesis may be consulted for the purpose of research or private study provided that due acknowledgement is made where appropriate and that the author's permission is obtained before any material from the thesis is published.

I agree that the University of Auckland Library may make a copy of this thesis for supply to the collection of another prescribed library on request from that Library; and

1. I agree that this thesis may be photocopied for supply to any person in accordance with the provisions of Section 56 of the Copyright Act 1994.

Or

- ~~2. This thesis may not be photocopied other than to supply a copy for the collection of another prescribed library.~~

*(Strike out 1 or 2)*

Signed: .....

Date: .....

Created: 5 July 2001

Last updated: 9 August 2001



# Abstract

Security of electronic patient health information(e-PHI) is emerging as a critical issue. In the United States, the Health Insurance Portability and Accountability Act(HIPAA) 1996 was passed to make protection of e-PHI a legal requirement for organisations that manage e-PHI. However the lack of specificity in its provisions raises uncertainty about their interpretations for any particular organisation.

In this thesis, we present the results of an exploratory investigation of security requirements under HIPAA, as perceived by the US dental schools for their enterprise dental information systems. This study was inspired by Software of Excellence Ltd, a NZ software vendor who exports enterprise dental information systems to the US market. It was experiencing difficulties developing appropriate security features for its products due to the lack of information about its customers' perceived security requirements under HIPAA. We used an online survey to elicit the perceived security requirements for enterprise dental information systems.

We used threat modeling as our main analytical framework for eliciting security requirements. Our survey instrument was designed to support analysis. The survey responses revealed some general perceptions held by the US dental schools regarding the security of their e-PHI and HIPAA. The survey also identified several security threats that the US dental schools were concerned about. We analyse these threats using a particular technique of threat modeling called the misuse case analysis. We conduct our analysis in the context of a model of a generic, enterprise dental information system which we define.

We propose improvements to the existing taxonomy of threats against e-PHI and classify our threats into the improved taxonomy. Finally we focus on one of the threats identified from the survey to propose mitigation.

# Acknowledgement

Firstly I would like to thank my supervisor, Professor Clark Thomborson. Without his expert advice and insight I would never have been able to finish this thesis. I gratefully thank him for his time and effort throughout the year.

I would like to thank Dr Gary Guest at the University of Texas for helping us with our survey design and administration.

I would like to thank Greg Allum at the Software of Excellence Ltd for his time and suggestions too.

I am also grateful to Barbara Thomborson for her suggestions for english language improvements of this thesis.

I also owe my family for their encouragement and support all year long.

Finally I thank my girlfriend Regina for her love and support.





# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Background . . . . .	1
1.2	Motivation . . . . .	4
1.3	Related Works . . . . .	5
1.4	Organisation . . . . .	6
<b>2</b>	<b>HIPAA Security Rule and Enterprise Dental Information Systems</b>	<b>7</b>
2.1	HIPAA Security Rule . . . . .	8
2.2	HIPAA Technical Safeguards . . . . .	9
2.3	Enterprise Dental Information System . . . . .	13
2.4	System Characterisation . . . . .	13
2.4.1	System Users and their Business Flows . . . . .	13
2.5	E-PHI . . . . .	15
2.5.1	Security Goals for e-PHI . . . . .	17
2.6	Discussion . . . . .	17
<b>3</b>	<b>Review of Security Requirement Engineering Methodologies</b>	<b>19</b>
3.1	Requirement Engineering . . . . .	20
3.1.1	Goal-based Methodologies . . . . .	21
3.1.2	Scenario-based Methodologies . . . . .	21

3.1.3	Viewpoint-based Methodologies . . . . .	22
3.1.4	Evaluation of Methodologies . . . . .	22
3.1.5	Techniques for Requirements Elicitation . . . . .	23
3.2	Security Requirement Engineering . . . . .	24
3.3	Threat Modeling . . . . .	27
3.4	Misuse Case Analysis . . . . .	28
3.5	Attack Trees . . . . .	30
3.6	Discussion . . . . .	31
<b>4</b>	<b>Existing Threat Taxonomy For e-PHI</b>	<b>35</b>
4.1	Threat Taxonomy For e-PHI in Existing Literature . . . . .	35
4.1.1	Levels of Organisational Threats . . . . .	36
4.1.2	Systemic Threats . . . . .	40
4.2	Countermeasures . . . . .	42
4.3	Discussion . . . . .	44
<b>5</b>	<b>Our Survey Methodology</b>	<b>45</b>
5.1	Data Collection Requirements . . . . .	46
5.2	Constraints . . . . .	46
5.3	Alternative Methods Of Data Collection . . . . .	47
5.4	Survey Instrument . . . . .	47
5.5	Survey Administration . . . . .	50
5.6	Sampling . . . . .	54
5.7	Response Rate . . . . .	55
5.8	Data Analysis Techniques . . . . .	55
5.9	Discussion . . . . .	56
<b>6</b>	<b>Results and Discussion</b>	<b>59</b>
6.1	Respondents . . . . .	59
6.2	General Findings . . . . .	60

---

6.2.1	Areas of Concern . . . . .	60
6.2.2	Perception about potential trade-off between security and patient care . . . . .	65
6.3	Threat Model From The Survey Responses . . . . .	65
6.4	Password Sharing by insiders . . . . .	68
6.5	Physical Theft of Desktop Computers that Store e-PHI . . . . .	71
6.6	Cover-up attempts by Insiders . . . . .	72
6.7	Disclosure of emails that contain e-PHI . . . . .	74
6.8	Unauthorised Access Through Unattended Workstation . . . . .	75
6.9	Data Inconsistency caused by multiple systems that are not integrated . . . . .	77
6.10	Clearinghouse breach that would draw us into investigation . . . . .	78
6.11	Suggested improvements to the existing taxonomy . . . . .	78
6.12	Misuse Cases Breakdown . . . . .	80
6.13	Discussion . . . . .	81
6.13.1	General Findings . . . . .	81
6.13.2	Misuse Cases . . . . .	83
<b>7</b>	<b>Mitigation for Coverup Attempts by Insiders</b>	<b>85</b>
7.1	Need for Audit Controls to Mitigate Coverup Attempts by Insiders . . . . .	86
7.2	Audit Controls . . . . .	86
7.3	Hypothetical Scenario of a Coverup Misuse Case . . . . .	87
7.4	Existing Requirements for Audit Controls . . . . .	88
7.4.1	HIPAA Provisions On Audit Controls . . . . .	88
7.4.2	RFC 3881 . . . . .	88
7.5	Detection of the Coverup Misuse Case using RFC 3881 . . . . .	90
7.6	Workflow-based Audit Controls for Countering the Coverup Misuse Case . . . . .	91
7.7	Discussion . . . . .	94
<b>8</b>	<b>Conclusions and Future Work</b>	<b>97</b>
8.1	Conclusions . . . . .	97

8.2 Future Work . . . . .	101
<b>A Survey Instrument</b>	<b>103</b>
<b>B Ethics Approval from the University of Auckland</b>	<b>109</b>
<b>C Raw Data From The Survey</b>	<b>113</b>

# List of Figures

2.1	HIPAA Structure . . . . .	8
2.2	Technical Safeguard Structure . . . . .	10
2.3	Typical user groups in a dental school . . . . .	13
2.4	Inter-organisational Flow of administrative E-PHI . . . . .	15
3.1	Security Quality Model . . . . .	24
3.2	The Security Engineering Process . . . . .	25
3.3	Security requirement engineering based on threat modeling . . . . .	26
3.4	Threat Modeling Process . . . . .	27
3.5	Example of misuse case analysis . . . . .	29
3.6	Example of attack tree modeling . . . . .	30
4.1	Two Categories of Threats against e-PHI . . . . .	36
4.2	Misuser groups for the five threat types . . . . .	37
4.3	Taxonomy of motives for organisational threats . . . . .	39
4.4	Flow of e-PHI through the health care industry . . . . .	40
5.1	First page of the online survey - Participant Information Sheet . . . . .	52
5.2	Second page of the online survey - Participant Consent Form . . . . .	53
5.3	Third page of the online survey - Survey Questions . . . . .	54
6.1	Mean Level of Concern for HIPAA Standards . . . . .	61

6.2	Overview of the misuse cases identified from the survey . . . . .	67
6.3	Password Sharing by a Student . . . . .	69
6.4	Password Sharing by a Faculty . . . . .	69
6.5	Physical Theft of Desktop Computers that Store e-PHI . . . . .	71
6.6	Cover-up attempts by Insiders . . . . .	73
6.7	Disclosure of emails that contain e-PHI . . . . .	75
6.8	Unauthorised access through an unattended workstation. . . . .	76
6.9	Data Inconsistency caused by multiple systems that are not integrated . . . . .	77
7.1	Workflow-based Detection of Coverup Misuse Case . . . . .	93
B.1	Page one of the Participant Information Sheet . . . . .	110
B.2	Page two of the Participant Information Sheet . . . . .	111
B.3	Participant Consent Form . . . . .	112

# List of Tables

2.1	HIPAA provisions for each standard of the Technical Safeguards . . . . .	11
2.2	Implementation Specification for HIPAA Standards . . . . .	12
4.1	Summary of countermeasures for organisational threats . . . . .	42
6.1	Survey Respondent Roles . . . . .	60
6.2	Abbreviations for the names of the HIPAA standards to be used in subsequent tables . . . . .	60
6.3	Levels of concern for each HIPAA standard . . . . .	61
6.4	Results of t-test between mean level of concern for audit control and the other standards . . . . .	62
6.5	Rank ordered responses for the level of concern for each standard . . . . .	63
6.6	Points assigned to each standard . . . . .	63
6.7	Results of second t-tests between mean level of concern for audit control and the other standards based on our rescaled point system . . . . .	64
6.8	Results of third t-tests between mean level of concern for Transmission Security and the other standards based on our rescaled point system . . . . .	64
6.9	Responses to the question on potential trade-off between security and patient care . . . . .	65
6.10	Raw data from the survey describing the security threats and corresponding misuse cases . . . . .	66



6.11 Taxonomic breakdown of the identified misuse cases . . . . . 81

7.1 Audit Trails for Hypothetical Coverup Misuse Case Based on RFC 3881 . . 90

C.1 Respondent Roles (Institutions were anonymised) . . . . . 113

# 1

## Introduction

### 1.1 Background

Security of electronic patient health information(e-PHI) is emerging as a critical issue as the healthcare industry becomes increasingly computerised. The term e-PHI refers to any electronic information relating to a patient's health, health care or payment for health care that is individually identifiable [1]. Other terms such as Electronic Medical Record(EMR) and Electronic Health Record(EHR) are also used often in the literature as synonyms. Cushman explains why security of e-PHI is important and how it is different from protecting traditional paper-based patient health information in [2]. He argues that health information of a patient often contains some of the most sensitive information about him/her. Thus it is an ethical belief inherent in our society that health information

belongs to the patient. We believe we have the right to control who accesses our health information. This fundamental right to privacy dictates that holders of our health information protect its confidentiality. Moreover the reported cases of discrimination based on one's health information in areas such as insurance or employment justify the importance placed on maintaining confidentiality [3]. While it is important to keep health information private, availability and integrity of health information in legitimate accesses by health practitioners can be the deciding factors between life and death for a patient. Thus confidentiality, integrity, and availability of patient health information is of great importance.

The shift to e-PHI from paper-based patient health information is happening because of the many advantages that e-PHI offers. It is expected to cut down the administrative costs of handling the voluminous paper records as well as enabling easier exchange of administrative and clinical information between healthcare organisations. The ultimate vision of e-PHI is to create a central repository of everyone's comprehensive, cradle-to-grave patient health information regardless of geographic location of patients. This has long been the 'holy grail' of healthcare IT development which is expected to bring enormous improvements in the quality of healthcare [4]. So in countries around the world, work is underway to develop components of e-PHI that will support such national infrastructure [5, 4].

However the increased level of sharing on top of the inherent qualities of electronic media make e-PHI more vulnerable to misuse. Cushman argues that providing security for e-PHI will be much more difficult because pieces of everyone's health history will reside in public and private computer repositories. He points out that while it is possible in theory to control and record access in electronic systems, once security is breached, damages can be on a larger scale than in paper systems. In fact, the security issues of e-PHI are one of the main factors slowing the adoption of e-PHI [6]. To address the unique challenge of securing e-PHI, countries are trying to make security of e-PHI a mandatory requirement by passing legislations and publishing standards that healthcare entities have to comply with [7].

In New Zealand(NZ) no statute specifically deals with security of ‘electronic’ patient health information. Instead ‘The Privacy Act 1993’ and ‘The Health Information Privacy Code 1994’ set out the legislative path to the privacy of patient health information in general [4]. Privacy is a slightly different concept from security although they are closely related and it is worth making the distinction here. Privacy concerns ownership and the controls that entail that ownership, whereas security is about protection against harm [8]. Nevertheless the guiding principles of the two privacy legislations motivated the development of the Health Networking Code of Practice which specifically details how to exchange e-PHI in a secure manner at policy level. In accordance with this Code of Practice, the NZ government developed the Health Intranet which is an implementation of a nation-wide health care network.

In the United States(US), ‘The Health Insurance Portability and Accountability Act 1996’(HIPAA) was passed to ensure adequate protection of e-PHI was a legal obligation for the covered entities while improving the efficiency of health care. It includes the Privacy Rule and the Security Rule for provisions of privacy and security respectively. The former covers the patient health information in both paper and electronic form whereas the latter applies only to e-PHI. HIPAA is a federal law so the covered entities will face severe fines and/or criminal prosecution if they are found to be in violation with the legislation. Therefore the covered entities have a strong motivation to comply. Huston claims that to date, HIPAA is the most organizationally motivating law that aims to provide security and privacy of e-PHI in the US [3].

In this thesis we present the results of an exploratory investigation of the security requirements for enterprise dental information systems under HIPAA, as perceived by the US dental schools. Software of Excellence Ltd(SOE), a NZ software vendor who exports enterprise dental information systems to the US dental schools market inspired this research. Greg Allum, who is the head of development in the company has pointed out the difficulty that they are experiencing in identifying the security requirements held by their customers regarding HIPAA [9]. In the next section we motivate this research further.

## 1.2 Motivation

As stated in Section 1.1 this research is motivated by difficulties experienced by a local software exporter who exports enterprise dental information systems to the US dental schools market. The company needed some insight into the security requirements under HIPAA as interpreted by its potential customers. It did not have any prior knowledge about the US dental schools' perceptions about HIPAA security requirements.

Because the deadlines for compliance with the HIPAA security rule have passed, the covered entities are scrambling to comply with the new provisions [10]. HIPAA certainly renewed the sense of urgency among the health care organisations to protect their e-PHI. However, compliance is proving a big challenge for many covered entities.

The main problem is the lack of specificity in the HIPAA provisions [11]. HIPAA does not prescribe implementation or advocates use of any particular technology. Instead it mandates the health care organisations themselves identify any reasonable threats and appropriate mitigation measures. This makes HIPAA applicable to a wide range of organisations that vary in terms of security needs and resources. Because of its lack of specificity however, the provisions are subject to interpretations by the health care organisations. This creates uncertainty among the health care organisations as to how to implement the various provisions. From the perspective of information system vendors who are not aware of their customers' perceptions this is clearly problematic as they have to design a system to the satisfaction of these organisations. In Chapter 2 we elaborate on this problem.

In this thesis we elicit security requirements held by the US dental schools for their enterprise dental information systems using an online survey. Our survey methodology is based on the threat modeling approach to security requirement engineering found in the existing literature. Based on the survey results, we firstly examine the general perceptions of the survey respondents regarding HIPAA and security of their e-PHI. Then we elicit more specific security requirements in the form of misuse cases which is a particular technique of threat modeling. We define a model of a generic enterprise dental information

system and analyse the misuse cases in the context of that model. We also attempt to classify the misuse cases according to an existing taxonomy of threats against e-PHI and propose improvements to the existing taxonomy based on our results.

Following the discussion of the misuse cases we focus on mitigating one of the misuse cases. We examine the ways in which a particular misuse case where a dentist alters e-PHI inappropriately to cover up for his/her mistakes can be countered. Finally we discuss how the existing guidelines for health care audit controls can mitigate the misuse case and propose improvements.

It is worth noting that this study focuses on the US dental schools who are only a small subset of the entities that manage e-PHI. We also make the point that our work is of exploratory nature. This thesis is intended to serve as a case study and its results to serve as guidelines for future investigations of similar kind on a larger scale.

## 1.3 Related Works

Security of e-PHI is an active area of research. Our review of the existing research efforts discovered a gap in the literature. There is a body of literature that takes a legal analysis approach to explain how legislative controls will affect health care. In the case of HIPAA, [12] is one such example. Typically this type of works explains the details of the legislation and analyse their implications on various aspects of health care.

Apart from those works that deal with impact of legal controls there are works that focus on legal compliance [10, 13]. They take a process centered view describing the necessary steps to achieve compliance. Other works concern themselves with the compliance status of the relevant organisations and the main obstacles that they are experiencing [14, 15].

All of the types of work discussed above provide only a brief and superficial coverage on the technical aspects of compliance. Research efforts that take a more technical perspective on the matter also exist. A wide range of technical solutions and their evaluations aimed to provide better protection of e-PHI can be found [16, 17, 18, 19].

In our search we found very little literature that is concerned with the perceptions about security requirements for health care information systems held by the health care organisations themselves. Implementation guidelines for each section of the HIPAA security rule are given in [11]. A set of technical best-practices for general e-PHI security is provided in [20]. A taxonomy of threats and a list of common threats against e-PHI are presented in [8] and [21] respectively. However their results are not based on the perceptions about the security requirements held by the health care organisations and they do not specifically concern HIPAA except for [11].

To our knowledge there was not any previous work that focused on the elicitation and analysis of the HIPAA security requirements for medical information systems as perceived and interpreted by the health care organisations themselves.

## 1.4 Organisation

Chapter 2 sets the context for our problem by outlining the relevant sections of HIPAA and characterising a typical dental information system. Chapter 3 reviews the existing methodologies for engineering security requirements and discusses how they can be used to solve our problem. Chapter 4 examines an existing taxonomy of threats against e-PHI. Chapter 5 describes our particular survey-based methodology. Other options for carrying out our research are evaluated and our design decisions are justified. Chapter 6 provides analysis of the survey results followed by discussion of our main findings. Chapter 7 examines potential mitigation measures for a particular security threat identified from the survey and makes recommendations. Chapter 8 summarises our work and draws conclusions as well as suggesting areas of future work.

# 2

## **HIPAA Security Rule and Enterprise Dental Information Systems**

In this chapter we further set the problem by providing relevant details. Since we used HIPAA as the basis of our investigation, in Section 2.1 and Section 2.2 we outline the relevant provisions of HIPAA. Then in Section 2.3 and Section 2.4, we characterise a typical enterprise dental information system. In Section 2.5 we discuss e-PHI and its security qualities that have to be protected by enterprise dental information systems.



## 2.1 HIPAA Security Rule

HIPAA is a massive legislation that covers many areas. The overall structure of HIPAA and the Security Rule can be found in Figure 2.1.

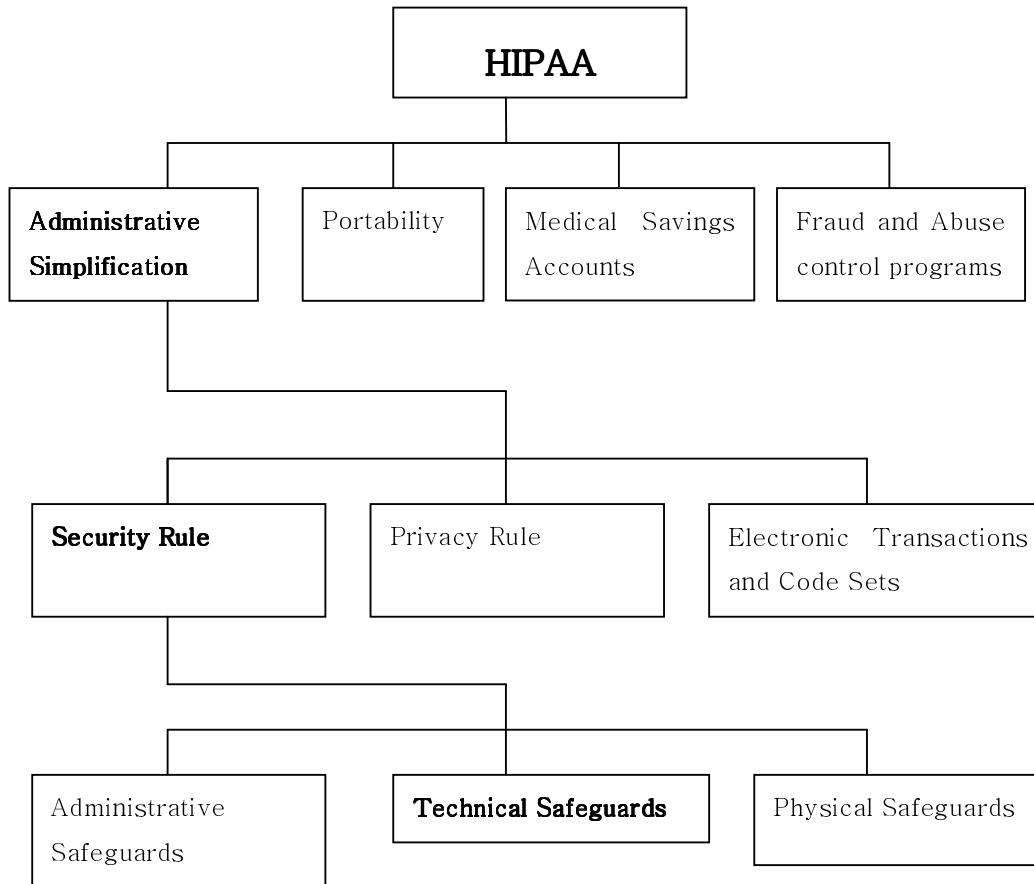


Figure 2.1: HIPAA Structure (Items in bold are the ones that this thesis will concern itself with)

Among many things HIPAA contains the ‘Administrative Simplification’ that aims to simplify the administration of healthcare in general. The Administrative Simplification in turn contains the Security Rule which is dedicated to the issue of e-PHI security. The Security Rule itself comes in three subsections called safeguards. The Technical Safeguards provide guidelines for necessary security features of the health care information systems. The Administrative Safeguards concern controlling the people and the business processes to ensure security. The Physical Safeguards try to physically secure the workstations and relevant storage devices. Thus all three safeguards are essential for a complete discussion of security of e-PHI. However due to time and resource constraints, we will consider

only the technical issues and compliance with the Technical Safeguards. Whereas given health care providers must implement appropriate physical and administrative safeguards, technical safeguards concern features of the information system and therefore are the realm of software vendors. Thus for our purpose of engineering security requirements for enterprise dental information systems, considering the technical safeguards will suffice.

It is worth describing the concept of covered entities before going further. HIPAA defines three types of covered entities(CE) who must comply with its provisions including the Security Rule [1].

1. Healthcare providers : Dental schools, doctors, hospitals, clinics, pharmacists, etc that transmit any personally identifiable health information in electronic form in connection with a person's healthcare.
2. Healthcare plans : An individual or group plan that provides or pays the cost of medical care.
3. Healthcare clearinghouses : Any entity that processes or facilitates the processing of e-PHI for a CE. This includes billing services and community health IT systems.

Covered entities exchange e-PHI with other CEs using standardised transactions and code sets which are also part of HIPAA. In the next section we discuss the HIPAA Technical Safeguards in more detail.

## 2.2 HIPAA Technical Safeguards

The Technical Safeguards are a set of requirements for information systems that manage e-PHI. Figure 2.2 shows the overview of the structure of the Technical Safeguards.

There are five standards in the Technical Safeguards.

1. Access Control - This is intended to enable setting of access privileges for users according to the organisational policy and making sure that the access control policy is not violated.

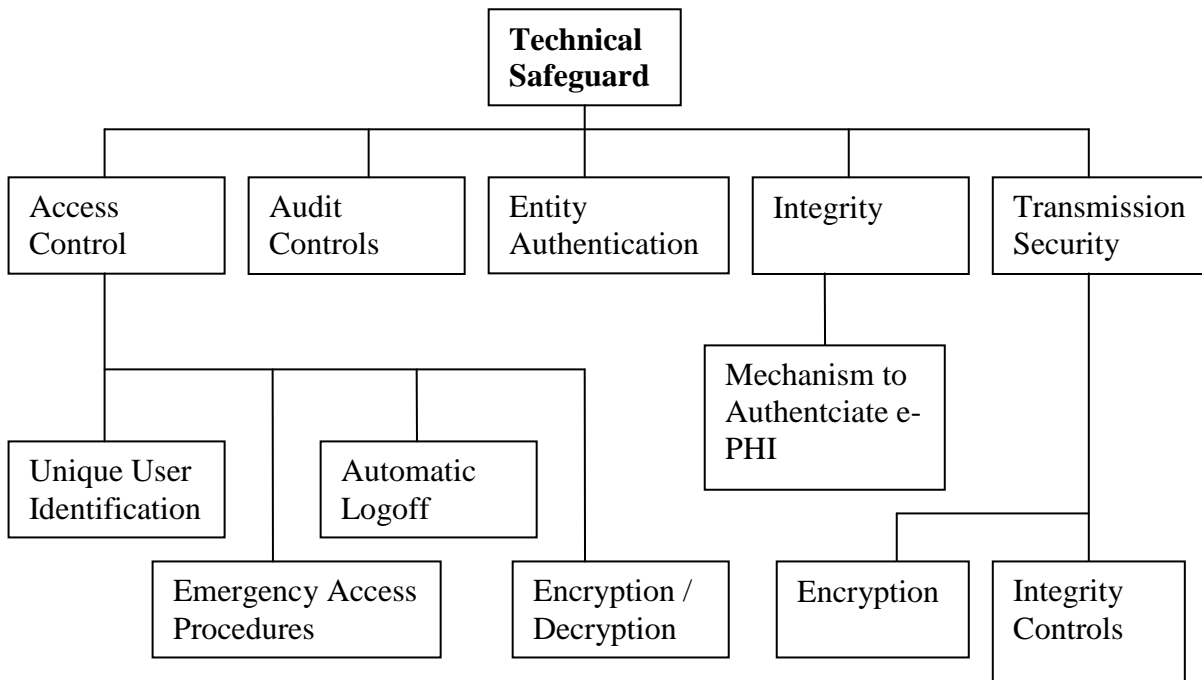


Figure 2.2: Technical Safeguard Structure

2. Audit Control - This refers to controls that enable the process of recording system activity and detecting misuses
3. Integrity - These controls ensure that data is not altered inappropriately.
4. Transmission Security - These controls protect information while it is in transit.
5. Entity Authentication - These controls ensure that only the legitimate users are let in to the system.

Access Control, Audit Control and Entity Authentication are security controls commonly found in other security literature whereas Integrity and Transmission Security are not. In Section 4.2 we compare the standards with a taxonomy of security mechanisms for e-PHI, proposed prior to HIPAA and discuss the similarities and differences.

Table 2.1 shows quotations of how each standard is defined under HIPAA taken from [1].

It can be seen that the standards are specified at the level of general principles. They do not provide any specific threat model to protect against or architectural/implementation level recommendations. However some implementation level specifications are available

Table 2.1: HIPAA provisions for each standard of the Technical Safeguards (adapted from [1])

Standard	Definition
Access Control	“Implement technical policies and procedures for electronic information systems that maintain electronic patient health information to allow access only to those persons or software programs that have been granted access right”
Audit Control	“Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain electronic patient health information”
Integrity	“Implement policies and procedures to protect electronic patient health information from improper alteration or destruction”
Entity Authentication	“Implement procedures to verify that a person or entity seeking access to electronic patient health information is the one claimed”
Transmission Security	“Implement technical security measures to guard against unauthorised access to electronic patient health information that is being transmitted over an electronic communications network”

for Access Control, Integrity and Transmission Security standards. An implementation specification is either required or addressable. Required means that the CEs must comply with the given implementation specification. Addressable means that the CEs can meet implementations by alternative means as long as they document their decisions adequately [11]. We provide the quotations for the implementation specifications taken from [1] in Table 2.2.

The separation between required and addressable types of implementation specifications allows more flexible application of the provisions. Covered entities have varying levels of risks and available resources. Required specifications are the minimum set of requirements for which no alternatives would offer the same level of security. For example unique user identification involves assigning an unique ID to every system user. Any alternative methods of identifying users such as role-based user identification will adversely impact on the overall security of the system by offering a much lower auditability.

In contrast addressable specifications are controls for which there are alternatives. For example there are many ways in which data can be encrypted and decrypted. Let’s con-

Table 2.2: Implementation Specification for HIPAA Standards

Standard	Implementation Specification
Access Control	Unique User Identification (Required) - "All users must be uniquely identifiable within the information system"
	Emergency Access Procedure (Required) - "Emergency access should be supported by the information system"
	Automatic Logoff (Addressable) - "The information system should log off automatically after a fixed time when there is no activity"
	Encryption Decryption (Addressable) - "Capability to encrypt and decrypt e-PHI should be supported by the information system"
Integrity	Mechanism to authenticate e-PHI (Addressable) - "Electronic mechanisms must be implemented to corroborate that e-PHI has not been altered or destroyed in an unauthorised manner"
Transmission Security	Integrity Controls (Addressable) - "Implement security measures to ensure that electronically transmitted e-PHI is not improperly modified without detection"
	Encryption Controls (Addressable) - "Implement a mechanism to encrypt e-PHI whenever deemed appropriate"

sider private and public key encryptions. In situations where secure key exchange can be assured, private key encryption may be more appropriate whereas public key encryption would be more suitable when there is no such assurance. Also the two alternatives have different requirements as to the computational resources. Therefore the choice of a particular encryption technology by a CE will depend on a variety of organisational factors including risk levels, security context and resource availability. Thus the combination of required and addressable implementation specifications make HIPAA more applicable to a wide range of CEs.

The high level of applicability comes at the expense of specificity. It can be seen that even the implementation specifications, especially the addressable ones are phrased in a way that does not prescribe detailed implementation. Instead it is the task of each dental school to carry out thorough risk analysis to determine exactly what they need in their information systems. In the next section we describe a generic, enterprise dental information system for dental schools.

## 2.3 Enterprise Dental Information System

Wikipedia defines the term ‘enterprise information system’ as “any kind of computing system that is of enterprise class. This means typically offering high quality of service, dealing with large volumes of data - capable of supporting some large organization” [22]. For our purposes, we define enterprise dental information system to be a specific kind of computing system which supports all aspects of a dental school’s clinical and administrative business processes.

## 2.4 System Characterisation

In this section we characterise various aspects of an enterprise dental information system. Our characterisations are based on the product manual of the SOE Ltd’s dental school product [23]. We identify the main system user groups and their typical business flows that an enterprise dental information system has to support. We believe that our characterisations are generic enough that they can be applied to other similar systems.

### 2.4.1 System Users and their Business Flows

Figure 2.3 shows the main user groups in a typical dental school.

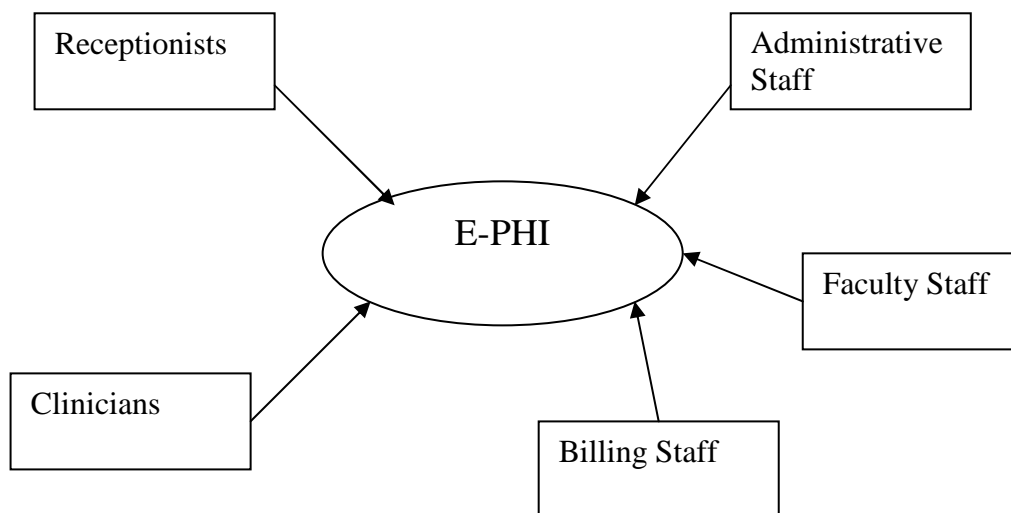


Figure 2.3: Typical user groups in a dental school

In the following subsections we explain each user group's responsibilities and identify a typical business flow.

### **Billing**

Billing staff are responsible for arranging payments and making sure insurance claims are processed correctly with the healthcare plans in a timely manner. Therefore they are authorised to initiate and receive transactions involving e-PHI. An example of a typical business process is submitting and viewing insurance claims.

### **Receptionists**

Receptionists are responsible for managing patient details and appointments. An example of a typical business process is managing patient appointments.

### **Clinician**

Clinicians are responsible for providing the actual dental care. An example of a typical business process is recording oral diagnosis. In a dental school environment clinicians include students who are not yet fully qualified yet. They need signoff from designated faculty members.

### **Faculty members**

Faculty members are responsible for management of academic aspects of a dental school. They manage student assignments and grade works completed by students. An example of a typical business process is assigning patients to students. Faculty members might need to access some e-PHI when assigning patients to students. However it is important to note that faculty members themselves are often the clinicians who provide care to patients.

### Technical Administrator

Administrator level users are responsible for the overall proper functioning of the system. An example of a typical business process is setting up user accounts. Technical administrators often have the privilege to set up users and corresponding access rights so in theory they can access e-PHI although they might not need to.

## 2.5 E-PHI

In this section we discuss e-PHI and its security qualities which have to be protected by an enterprise dental information system. E-PHI is the most important asset that needs to be protected by a dental information system. E-PHI of a patient comes in two parts.

Clinical data is data that directly supports care given by health providers. In a dental care context, it can include things like treatment history, oral diagnosis report and oral x-ray charts. Administrative data is data that indirectly supports care given by health providers. Patient demographics and insurance related data are the main types of administrative data.

Exchange of administrative data was simplified a great deal by the passing of HIPAA. HIPAA's transactions and codesets mostly revolve around sharing insurance related data [24]. Figure 2.4 shows the exchange of administrative e-PHI between the HIPAA CEs.

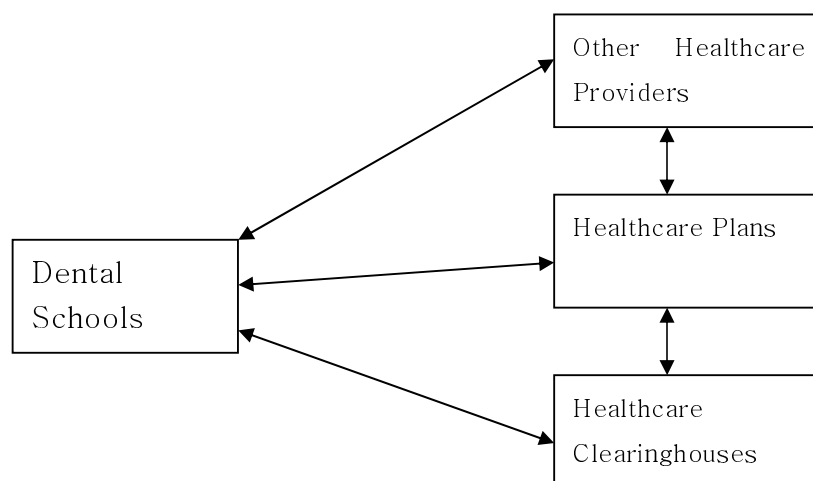


Figure 2.4: Inter-organisational Flow of administrative E-PHI



Dental schools communicate administrative data to and from insurance companies, clearinghouses and other dental providers. Transfer of administrative e-PHI occurs using codesets and transactions specified in HIPAA [24]. Well-known electronic data interchange standards such as X12 and HL7 are used for implementation of the codesets and transactions. An enterprise dental information system should therefore support these communication functions.

On the other hand, Brailer et al. claim that the majority of health care industry is still very fragmented as far as the clinical data is concerned [5]. They argue that new medical technologies are constantly changing what is in the clinical data. This makes sharing of clinical data much more difficult. However, easy sharing of clinical data among the care providers is expected to result in huge improvements in the quality of care. So in the US efforts are under way at the regional levels to create common repositories of clinical e-PHI called health information exchanges [5, 25]. These current efforts to share clinical data take the approach where some central repository of e-PHI is created by merging databases of multiple health care organisations. This is in contrast with the electronic data interchange type sharing of administrative data where relevant data is codified and exchanged between organisations using defined transactions with no such central storage. We believe that this difference is due to the high variability of the format and content of clinical data which makes it more difficult to codify than administrative data. Our dental information system does not concern itself with the sharing of clinical e-PHI with external systems.

Each of the user groups identified in the Section 2.4 has varying amount of access to clinical and administrative portions of e-PHI. For example, clinicians are likely to have full access to clinical data while having restricted access to administrative data. Billing staff on the other hand will have access to all the insurance related data while not having access to the clinical data.

### 2.5.1 Security Goals for e-PHI

The ISO/DIS 27799 which is the draft international standard for security management in health informatics, states that confidentiality, integrity and availability are the main security goals for health care information [21]. A secure dental information system must implement appropriate technical controls as outlined in HIPAA Technical Safeguards to preserve these three security qualities of e-PHI.

## 2.6 Discussion

We examined the security requirements for an enterprise dental information system imposed by the Technical Safeguards of the HIPAA Security Rule. The Administrative Safeguards and the Physical Safeguards deal with the aspects of e-PHI security that are outside the boundaries of an information system and therefore were omitted from our analysis. The Technical Safeguards specify five broad categories of security mechanisms for adequate protection of e-PHI, namely Access Control, Transmission Security, Audit Control, Integrity and Entity Authentication. However, the actual provisions show that they lack specificity in terms of how to implement each standard. Although some implementation specifications are available for three of the standards, the majority of them are addressable which means that they can be met through alternative means. While this lack of specificity increases applicability of the legislation, it makes the provisions subject to interpretations by the CEs.

We defined what we mean by the term enterprise dental information system and characterised various aspects of a typical system such as user groups and their main business processes. We identified e-PHI and its security goals as the main assets that our enterprise dental information system must protect while supporting the business flows of its users. The two different portions of e-PHI, namely clinical and administrative were identified. Depending on their business flows some user groups need access to the clinical part of e-PHI whereas some need access to the administrative part of e-PHI. We found that the current level of sharing for clinical and administrative e-PHI among the health care or-

ganisations differs. HIPAA defines transactions and codesets to facilitate easy sharing of administrative data but it does not concern sharing of clinical data. High variability of clinical data due to the diverse and fast-changing nature of health care industry leads to difficulties in codifying it for the kind of exchange being used for administrative data. Although efforts are underway to create regional repositories of clinical data that would enable easier sharing, the level of sharing for clinical data is still relatively low. We made the assumption that our dental information system supports the exchange of administrative e-PHI but it does not concern itself with the sharing of clinical e-PHI.

Nonetheless our dental information system should protect both types of e-PHI. We identified the three primary goals for e-PHI security which are confidentiality, integrity and availability. To ensure that these goals are met, the job of an enterprise dental information system is to appropriately implement the five standards of the HIPAA Technical Safeguards. As it is up to the individual CEs to interpret the legislation and come up with appropriate implementations, their requirements are an important consideration for information system vendors in designing their products. Therefore from the perspective of information system vendors it is important to elicit these interpreted requirements held by the CEs. In the next chapter we review the existing methodologies for engineering security requirements and evaluate their suitability as the analytical framework for our study.

# 3

## **Review of Security Requirement Engineering Methodologies**

In this chapter we review the existing methodologies for security requirement engineering and evaluate their relevance to this thesis. In Section 3.1 we review the general requirement engineering literature. Then in Section 3.2 we specifically examine the existing methodologies for security requirement engineering. In Section 3.3 we discuss ‘threat modeling’ which is a particular approach to engineer security requirements. In Section 3.4 and Section 3.5, we examine two existing techniques for threat modeling, namely misuse case analysis and attack trees.

### 3.1 Requirement Engineering

Requirement engineering (RE) is often the first phase of a software development project. Software requirements specify the behaviour of a software system. Nuseibeh et al stress the importance of good requirements by arguing that the primary measure of success of a software system is the degree to which it meets the intended purpose [26]. Zave provides a definition of RE which Nuseibeh et al. considers to be one of the clearest [27]: “Requirements engineering is the branch of software engineering concerned with the real-world goals for, functions of, and constraints on software systems. It is also concerned with the relationship of these factors to precise specifications of software behavior, and to their evolution over time and across software families.”

In Zave’s definition RE is an extensive process that continues throughout the lifecycle of a software system. According to this definition there are three factors that drive the RE process. Firstly there are goals that fundamentally motivate software systems. These goals necessitate the functions of a software system that will achieve them. The functions, in turn, must be qualified by the various constraints which are referred to as non-functional requirements. A RE methodology specifies how to carry out the various activities in an RE effort.

For our purposes, we need an RE methodology that involves the users because we want to elicit requirements held by the US dental schools. In this light we looked for approaches that involve the users from the early stages of the RE process. The need for actively involving the users in the RE process is well recognised in the RE literature. Nuseibeh et al argue that requirements engineering almost always takes place in the context of a human activity system. The underlying purpose of conducting RE is to solve some problem owned by people. Therefore requirement engineers need to be sensitive to how people perceive and understand the world around them. Goguen also advocates this notion by arguing that the problems of requirement elicitation cannot be solved without considering the social context [28]. Moore stresses the importance of end-user interaction by arguing that the end-users are the ones who will interact directly with a given system

so it is vital that system meet their expectations [29]. Therefore it is a major goal early in the software engineering process to gather meaningful requirements from end-users. The more rigorous, formal modeling approaches do not require the user perceptions or understandings [30, 31]. However, such methods are considered to be complementary methods rather than replacements to the methodologies that are driven by the users. From our literature review we identified three broad categories of software requirement engineering methodologies that incorporate this idea, namely goal-based, scenario-based, and viewpoint-based.

### 3.1.1 Goal-based Methodologies

Goal-based requirement engineering refers to the process of gathering and analysing requirements from user goals. Goals denote the objectives a system must meet [26]. The KAOS methodology is an example where ‘goal’ is the central concept in requirements acquisition [32]. Lamsweerde argues that goal-oriented RE ensures that operational requirements meet various objectives of a system such as safety and security. In goal-based RE methodologies, goals are used as the main guiding concept in developing requirement specifications [33]. Often the stakeholders have only a vague idea of what their system should do or should not do. These fuzzy ideas can be modeled as some user goals. These abstract, high level goals are then refined into sub-goals, and so the process continues until they are detailed enough to be mapped to technical implementation.

### 3.1.2 Scenario-based Methodologies

While goals are of critical importance, it is often the case that users have trouble articulating their goals [26]. In such cases the tasks that users currently perform and those that they might want to perform can be used to detect user requirements. These instances of experience/interaction with a system captured from users are called scenarios [34]. Scenario-based RE methodologies drive the RE process by eliciting and analysing various user scenarios. The inquiry cycle proposed by Potts is an example of a scenario-based

RE methodology. Traditional use case modeling is another example of a scenario-based approach.

### 3.1.3 Viewpoint-based Methodologies

Viewpoint-based RE methodology emphasizes perspectives of the various stakeholders for the system. In [26], the stakeholders are described as “individuals or organisations who stand to gain or lose from the success or failure of a system”. Each stakeholder will have his/her own set of goals and functions that may conflict with others’. A viewpoint-based RE methodology recognises the need for resolving discrepancies between various stakeholders and provides ways to settle them [35].

### 3.1.4 Evaluation of Methodologies

It is worth noting that although differences exist in the orientation of the RE processes, the underlying concepts such as goals, scenarios, and viewpoints are crosscutting concerns used in all three categories. In fact in real life situations they are often used together to complement each other [35, 34]. Such an integrated approach where more than one methodology is used together is desirable, but it would often be too time-consuming. The choice of which type of methodology to use for a given situation will depend on the method of data acquisition, the scope of analysis, and the available timeframe. The goal-based approach seems to be a feasible option for this thesis. It would be possible to model the U.S. dental schools’ goals regarding the security of their e-PHI. However, as mentioned in Section 3.1.2, users often have difficulty articulating the goals themselves. In this regard the scenario-based approach would be a better option for our purpose because users can more easily identify use scenarios than goals in general. The viewpoint-based approach requires analysis of various stakeholders in the system. For a complete set of requirements, consideration of multiple viewpoints is inevitable. However, given the time constraints of this particular investigation we think that it will be infeasible to consider multiple viewpoints that exist within the dental schools. Therefore we believe that the

scenario-based RE methodology is best suited for our purposes.

### 3.1.5 Techniques for Requirements Elicitation

Whether it is goals, scenarios, or viewpoints, they need to be elicited using an elicitation technique. Nuseibeh et al. propose a taxonomy of four requirement elicitation techniques in [26] - *traditional techniques*, *group elicitation*, *Prototyping*, and *specialised approaches*. *Traditional techniques* include interviews, user surveys, and analysis of existing documentation. These are generic techniques that are widely used for data gathering in a variety of domains. While *group elicitation* techniques are similar to user interviews, they involve multiple stakeholders as in a workshop. They are useful when a consensus is needed among the various stakeholders. *Prototyping* is a technique that is often used when too little is known. A prototype can be used to obtain early feedback from the stakeholders. Lastly, *specialised approaches* include model-driven techniques, cognitive techniques, and contextual techniques such as protocol analysis and discourse analysis.

Interviews allow more direct interaction with the users compared to the surveys, but they require the requirement engineer to be present with the interview subjects. Because of this, it is relatively difficult to interview a large number of subjects compared to the number reached in a survey. Group interviews are a good way to form a consensus among multiple stakeholders, but they need more time. *Prototyping* is a viable technique when too little is known, but it has the danger of imposing the requirement engineer's understanding on the stakeholders thereby affecting their perceptions. Specialised techniques such as protocol analysis are promising, but they require much more in-depth study of the subjects.

In the next section we will review some more specific literature on security requirement engineering.



## 3.2 Security Requirement Engineering

We presented a brief overview of requirement engineering in general in Section 3.1 and Section 3.1.5. Although the general concepts of RE discussed in these previous sections still apply to security requirement engineering (SRE), they do introduce some unique challenges, too. In this section we will review some of the existing literature on SRE. It draws from several different research areas such as RE, information security, and business process management.

Historically research on SRE has received relatively little attention because much of the research on security concentrated on development of numerous security mechanisms [36]. In the RE literature security requirements are often regarded as a type of non-functional requirements that specify the various constraints on a software system [26]. Firesmith claims that unlike functional requirements, it is possible to use parameterised templates for security requirements [37]. According to Firesmith because security requirements are a type of quality requirement, they should be based on an underlying quality model. Thus security can be delineated into a hierarchical structure of quality subfactors as shown in Figure 3.1.

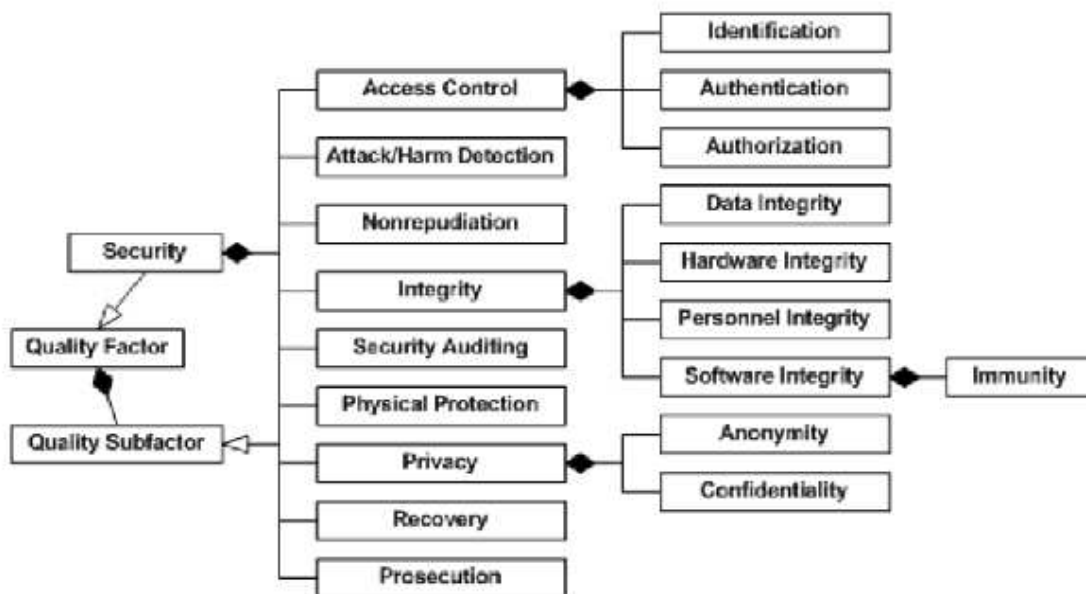


Figure 3.1: Security Quality Model (reproduced from [37])

Functional requirements can vary drastically from system to system. Firesmith argues

that with security requirements, however, the security quality sub-factors shown in Figure 3.1 will not change, and therefore it is possible to reuse them by parameterising the subfactors. However, the notion of reusable templates should not be used as a justification to leave security requirements until late in a development effort. Mead et al. points out the problem with the current industrial tendency of leaving security requirements until late in a development project despite the realisation that good requirements are critical to success [38]. They argue that a separate engineering effort that starts along with the functional requirements is required for security requirements. In fact, studies suggest that upfront inclusion of security requirements can result in savings of up to billions of dollars. In this light they proposed the Security Quality Requirement Engineering (SQUARE) methodology as a solution to the problem incorporating security requirements early in the software development cycle.

Similar to [38], there is a body of literature that takes the view that engineering security requirements need a specialised effort separate from the normal software engineering activities. Microsoft's guide on security engineering explains in detail how security-related activities should be carried out [39]. Figure 3.2 shows the normal software engineering process along with the corresponding security-specific activities.

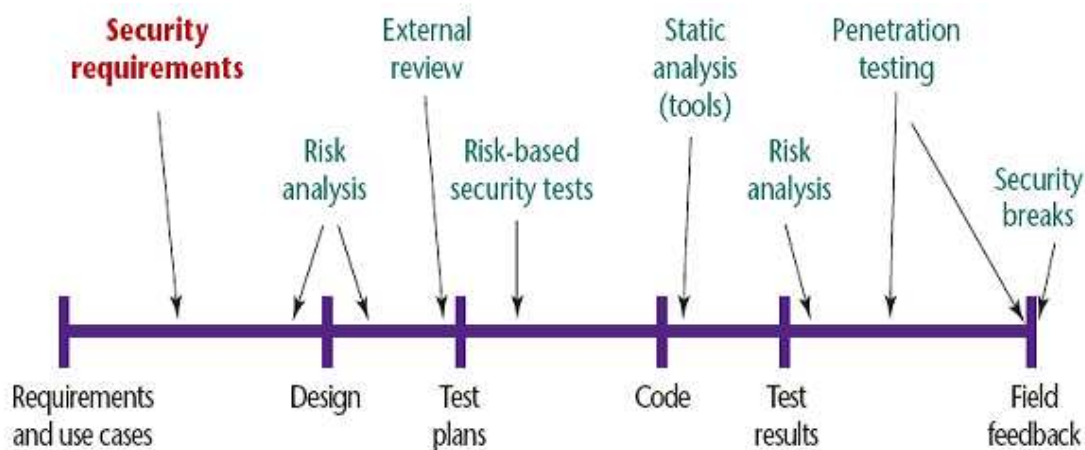


Figure 3.2: The Security Engineering Process (reproduced from [39])

In this figure security requirements is the first item in the security engineering process, and it happens during the specification of functional requirements. Thus it shows that elicitation of security requirements is just as important as the functional requirements. As

mentioned in our evaluation of the RE methodologies in Section 3.1.4, we decided that the scenario-based methodology is best suited for this study. However, traditional scenario-based methodologies such as use-case analysis are ineffective for security requirements. The reason for this is that while functional requirements are stated in terms of what must happen, security requirements are specified in terms of what should not happen [40]. Thus a scenario-based RE methodology designed for functional requirements lacks the capability to model negative scenarios that the system should not allow.

Threat modeling is a specialised scenario-based RE methodology that models these negative scenarios as ‘security threats’ and uses them for security requirements. The specific works on security requirements often point out the need for good threat modeling. Alexander argues that what is unique about security requirements is that they exist because of security threats [41]. Firesmith also argues that security requirements are driven by the security threats, and therefore the first task of security design should be the identification of the threats [37]. The very need for security in any situation is based on the fact that there are threats against some asset that we wish to protect. Myagmar et al. argue that threat modeling should be used as the basis for engineering security requirements. Figure 3.3 describes the security requirement engineering process starting from threat modeling.

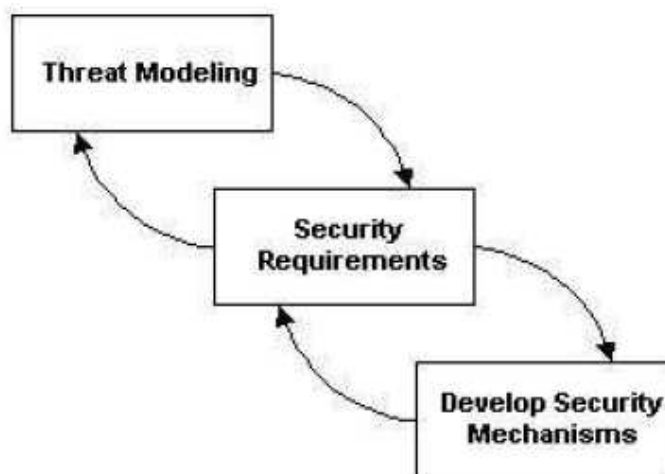


Figure 3.3: Security requirement engineering based on threat modeling (reproduced from [40])

Threat modeling leads to security requirements which are satisfied by the various

security mechanisms. In the next section, we will describe the threat modeling process in more detail. Then we will review two distinct threat modeling methodologies-misuse cases and attack trees.

### 3.3 Threat Modeling

According to [40] the threat modeling process consists of three phases that are shown in Figure 3.4.

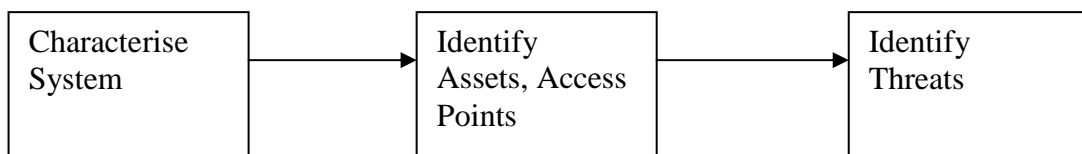


Figure 3.4: Threat Modeling Process (reproduced from [40])

The first phase of the threat modeling process is system characterisation. For detailed threat modeling there must be a system context. Thus the system in question must be characterised first. This includes understanding the data flow both within and outside the system. The main user groups and their use cases need to be taken into account as well.

Identifying assets and access points is the second phase in the threat modeling process. An asset refers to a resource of a system that must be protected from misuse. An asset is not necessarily tangible. It can refer to more abstract concepts such as data consistency which often are the security goals of a system. For a threat there will always be an asset in danger because they are the threat targets. Access points are what the attacker is going to use to gain access to the assets. In Chapter 2 we presented the first two steps of the threat modeling process by characterising our enterprise dental information system and identifying the e-PHI and its security goals.

Once the previous two steps are completed, then real threats can be modeled. Myagmar et al. suggest an approach where one starts this phase by considering the known threats already identified for similar systems and then going into more specific threats for the system in question using the information gathered in the previous phases. Another

way to enumerate threats also suggested by Myagmar et al. is to go through each of the system assets and create threat hypotheses that could violate confidentiality, integrity, or availability of the asset. It is worth noting that these authors' suggestions do not include any method where the end-users are asked about the threats that they are concerned about, which is what we need.

The threat modeling process would result in a threat profile for the system in question. Nonetheless a mere enumeration of potential threats is not useful unless they are analysed in the context of the system established in the previous two steps. In the literature there are techniques aimed at assisting this third step. In the following section we will discuss two such techniques, misuse case analysis and attack trees and then look at how threat models can be mapped to security requirements.

### 3.4 Misuse Case Analysis

Misuse case analysis is a recent development in SRE research that reverses the famous use case analysis to model security threats. Abuse case is another term often used in the literature, and it can be considered a synonym. The problem with use cases is that they do not provide good support for capturing non-normative behaviour of a software system [42]. To design a secure software system it is necessary to anticipate such non-normative behaviour. In essence misuse case is a negative scenario of system use that is potentially harmful to the system. Alexander defines a misuse case as a 'use case from the point of view of an actor hostile to the system under design' [41]. Misuse case analysis adopts the semantics and diagrammatic representation of the use cases. A misuse case models information regarding misusers and their actions and relationships with other misuse cases/use cases.

Alexander advocates an approach where misuse cases and use cases are used together to conduct security requirement analysis. Figure 3.5 adopted from [41] demonstrates this approach.

In the above example 'drive the car' is the system level use case. Then there is

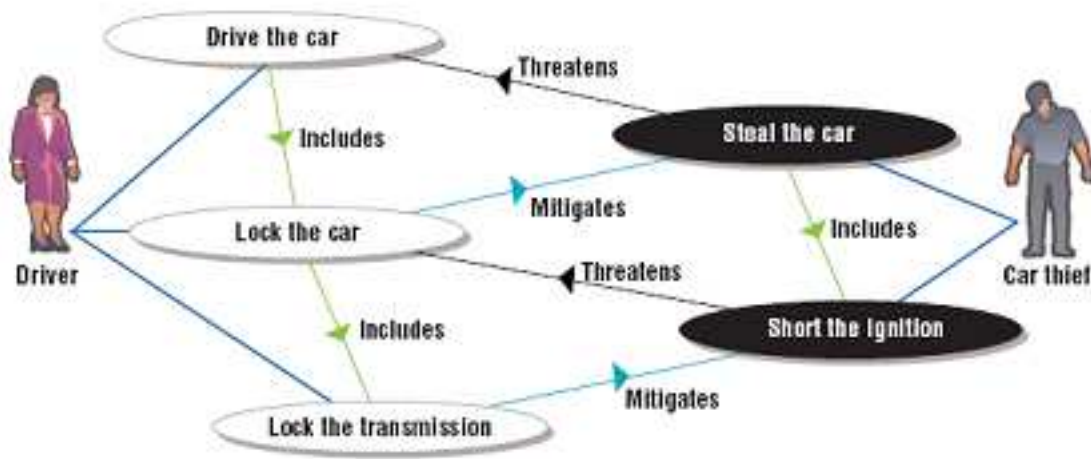


Figure 3.5: Example of misuse case analysis (reproduced from [41])

a system level misuse case, namely ‘steal the car’, which threatens the use case. To mitigate the misuse case the driver ‘locks the car’ which is threatened again by the next level misuse case, ‘short the ignition’. Thus the process is recursive going from the system level misuse cases to more detailed subsystem level misuse cases. Through this process of recursive interplay between use cases and misuse cases, Alexander claims that useful security requirements can be elicited.

The benefit of using misuse case analysis is that it does not require any rigorous mathematical analysis which can be time-consuming. Instead it offers a much more intuitive and informal way of engineering security requirements. Creation of useful misuse cases often takes place in the form of informed brainstorming [42]. Designers of the system and security analysts work together in this phase to develop real and interesting misuse cases. Various tasks can be undertaken to achieve this. Sometimes a systematic approach is taken where all the software/hardware/user interfaces of a system are carefully reviewed from the point of view of an attacker. Other times, a more heuristic approach is used where the security analyst simply tries to anticipate the attacker’s moves. During our review of the existing literature on misuse cases we did not find any methodology where misuse cases are elicited from the user concerns and perceptions.

### 3.5 Attack Trees

Attack trees are another way of eliciting security threats [43]. Designers use a tree structure to model security threats. Figure 3.6 shows an example attack tree for a safe.

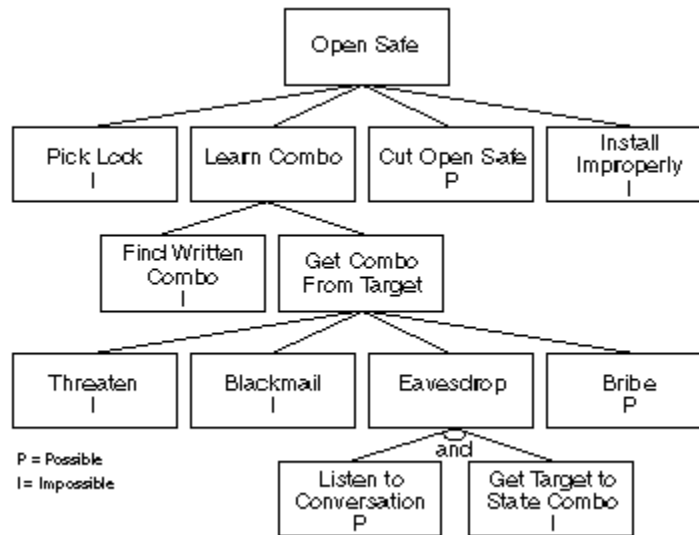


Figure 3.6: Example of attack tree modeling (reproduced from [43])

The goal of the attacker is the root node of the attack tree. The children nodes of the root node represent the ways in which the attacker's goal can be achieved. As we go down deeper into the tree structure, more detailed attacks are revealed. Also note that there are 'AND' and 'OR' nodes. In the example given in Figure 3.6, 'OR' nodes are default and 'AND' nodes are specified as so. So the four children nodes of the root nodes are 'OR' nodes. This means that if any one of the four children nodes is satisfied then the parent node is satisfied. Besides, attack trees provide ways to assign values to the leaf nodes to enable evaluations of different attacks. In the above example, node values are 'possible' and 'impossible'. However, it is equally possible to assign continuous values to the nodes such as probability of success of a given attack. Schneier claims that by using node values the security engineer can evaluate threats in terms of various factors [43].

To create attack trees, possible attack goals have to be identified. Each goal will result in an attack tree of its own. Then it is up to the security engineer to think of all possible attacks under each goal. This process must be repeated down the tree until there are no further children nodes to add. Schneier argues that although this approach can result

in some attack that is not thought of, it is the case with any security analysis, and thus creating attack trees takes practice. [44, 45] provide case studies of applying the attack tree methodology. Attack trees provide a way for the security requirement engineer to think about the different ways in which an attack can be mounted on a system. The methods of creating useful attack trees described in the literature are mostly driven by the security engineer. We did not find any work where attack trees were constructed based on an investigation of the user perceptions.

## 3.6 Discussion

In this chapter we reviewed the existing security requirement engineering methodologies. We firstly examined the general requirement engineering methodologies. In the general RE literature, understanding of user perceptions is considered a crucial part of the RE process. We identified three broad categories of RE methodologies that attempt to elicit the user requirements in various forms. Goal-based approaches focus on the user goals to better understand the user requirements. They seem to follow naturally from the fact that user requirements are fundamentally based on some goals that need to be achieved. The main drawback of goal-based methodologies is that the users are not accustomed to think in terms of their goals. Scenario-based approaches elicit scenarios of system use instead of goals. The argument for this is that users are often better at articulating about their use scenarios. Viewpoint-based methodologies mainly concern achieving consensus on the requirements from the various stakeholders for a given system. While such consideration of multiple stakeholders would eventually be necessary, for a pilot study it would be sufficient to consider one representative stakeholder within each dental school. Thus it seems that the scenario-based approach would be the best choice for our purpose.

However our examination of security requirements revealed their unique characteristics which make traditional methodologies ineffective. General RE literature often focuses on the functional requirements and gives less attention to security requirements. Scenario-based RE methodologies such as use case modeling are not suitable for engineering security



requirements because security requirements are stated in terms of what the users do not want. Thus in security requirement engineering the notion of security threat is used to represent these negative scenarios that users do not want. Threat modeling refers to the process of modeling the threats against a system. By identifying the threats and analysing them in the context of a particular system, security requirements can be elicited. Two specific techniques for threat modeling were examined, namely misuse case analysis and attack tree modeling.

For eliciting scenarios of normal system use, a variety of data gathering techniques are suggested. They range from traditional techniques such as surveys and interviews to more sophisticated techniques such as protocol analysis and discourse analysis. They all aim to gather user perceptions of their system use to aid in the RE process. However upon our review of the threat modeling literature, we found that suggested elicitation techniques for security threats are quite different. Instead of gathering user perceptions about security concerns, they mostly rely on the security requirement engineer to identify the security threats. The belief that an experienced security engineer is in a better position to identify potential threats is a possible explanation for this difference between functional requirements and security requirements. However, in our case where the goal is to study the user perceptions about security requirements, such reliance on the security engineer is inappropriate. We believe that one of the elicitation techniques widely used for functional requirements that gathers information from the users would be more suitable for our purpose. In our case the end-users are the dental schools who will ultimately be responsible for security of their e-PHI and legal compliance. Therefore we believe that it is important to understand their perceptions about the security requirements.

As for the analysis technique to be used once the security threats are gathered from the users, we compared misuse cases and attack trees. Attack trees are effective for refining and expanding abstract threats into more detailed attacks. They also provide ways to make comparisons between different threats by assigning them node values. But unlike misuse cases they do not explicitly model the attackers or model how the threats interact with the normal use of the system. Also diagrammatic notations of misuse cases

provide a visually effective way to communicate the threats. Another advantage of misuse cases over attack trees is the capability to include the mitigations as well as the threats themselves in the misuse case diagrams. Therefore we believe that misuse cases are the better alternative for our work.



# 4

## Existing Threat Taxonomy For e-PHI

From our review of the methodologies for engineering security requirements in Chapter 3, we identified threat modeling as a suitable approach. In this chapter we review an existing taxonomy of threats against e-PHI. In Section 4.1 we discuss the taxonomy in the context of our dental information system. In Section 4.2 we discuss the security measures for countering the threats identified in the taxonomy.

### 4.1 Threat Taxonomy For e-PHI in Existing Literature

In this section we review a taxonomy of threats against e-PHI proposed by the US National Research Council in [8].

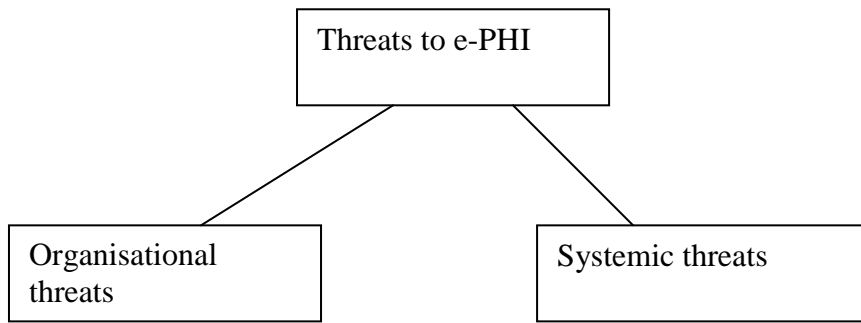


Figure 4.1: Two Categories of Threats against e-PHI

According to [8] there are two general categories of threats to e-PHI as shown in Figure 4.1. Firstly there are threats that directly violate the security policy of an organisation. These threats are called organisational threats. Since we cannot make definitive statements about security policies of individual organisations, we broadly assume that every security policy specifies confidentiality, integrity and availability of e-PHI that is within the organisational boundary as their security goals. This assumption is necessary to conduct our analysis in Chapter 6. Organisational threats occur due to authorised users who intentionally or unintentionally misuse their privileges or unauthorised outsiders who manage to break into the computer system. Secondly there are threats that arise from the various flows of e-PHI across the health care industry. These threats are called systemic threats.

#### 4.1.1 Levels of Organisational Threats

According to [8] there are five different types of organisational threats numbered from one to five. They are shown in the following list.

1. Threat 1(Accidental Misuse by Insiders): Innocent insiders who cause accidental breach of security by mistake.
2. Threat 2(Insiders abusing their access rights): Insiders who abuse their access rights. The attacker acts within the boundary of his/her access rights to commit the misuse.
3. Threat 3(Insiders going outside of their access rights): Insiders who go outside of their access rights and knowingly access information for spite or for profit. This

type of threat arises when an attacker does not have access to the desired data and through technical or other means gains unauthorized access to that data.

4. Threat 4(Unauthorised Physical Intrusion): The unauthorized physical intruder causing breach of security.
5. Threat 5(Unauthorised Technical Misuse): Rogue employees and outsiders, who mount attacks to the information system. This is a purely technical threat where the attacker has no authorization and no physical access.

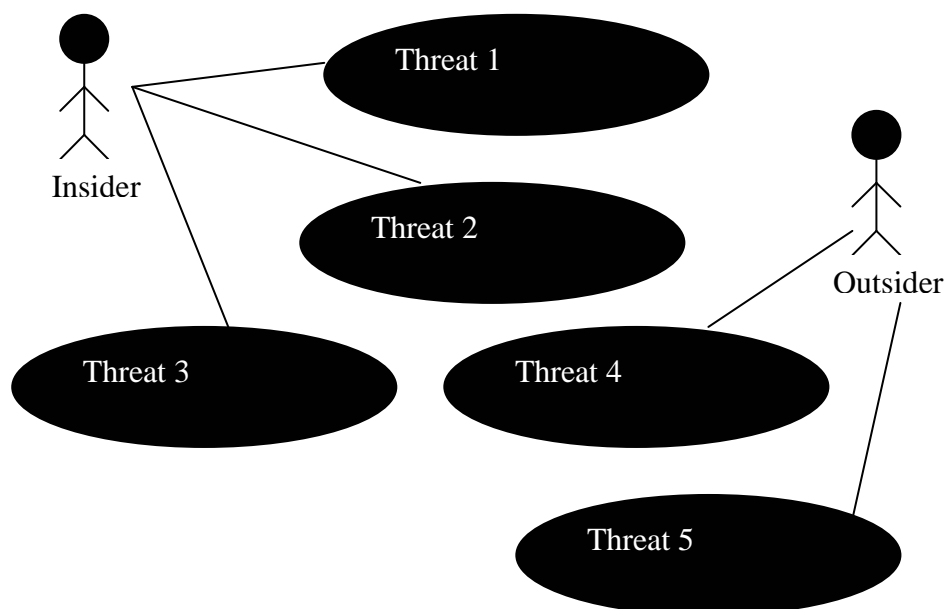


Figure 4.2: Misuser groups for the five threat types

Figure 4.2 shows that Threat 1, Threat 2 and Threat 3 types are committed by insiders whereas Threat 4 and Threat 5 types are committed by outsiders. The outside misusers differ from the inside misusers in that they do not have any authorisation to access e-PHI.

In the context of the system characterised in Section 2.3, any one of the user groups listed in Section 2.4.1 can potentially commit the Threat 1, Threat 2 and Threat 3 type misuses. Firstly Threat 1 type misuses lack the element of intent. However accidental misuse can violate confidentiality, integrity and availability of e-PHI just like the other types. For example, an innocent student who happens to read e-PHI of a patient on another student's screen by mistake is violating confidentiality by committing a Threat 1

type misuse. Similarly integrity and availability can also be compromised if a clinician alters or deletes e-PHI in an unauthorised manner by mistake. An accidental misuse can either occur within or outside the boundary of the access rights of the misuser. In the former case, the risk associated depends on the access rights of the user group to which the misuser belongs. We use the term access rights to refer to the data access rights as well as the permitted business flows for a particular user. An accidental misuse by a clinician who has full access to the e-PHI of a particular patient is more likely to incur more damage compared to such misuse by a billing staff who only has limited access rights. Thus more privileged user groups are more vulnerable to this type of accidental misuse. On the other hand, consider the latter case where the accidental misuse occurs outside the boundary of the access rights of the misuser such as the previous example where a student accidentally reads e-PHI present on his/her friend's screen. In such cases, the extent of breach is not so dependant on the user group of the misuser.

Unlike the Threat 1 type, Threat 2 type misuses are not accidental. This type of misuses are committed by the insiders who have the intent to harm the system. The important qualification here is the misuser is acting inside the boundary of his/her access rights. Similar to our analysis of the Threat 1 type, with Threat 2 type misuses the user groups with greater access rights will pose greater threats to e-PHI. Whatever the motive is, a misuse committed by a faculty member is likely to be more damaging than by a student.

Threat 3 type misuses are similar to Threat 2 type in that the misuser possesses intent to harm. However in Threat 3 type misuses the misuser is acting outside his/her access rights to gain unauthorised access to e-PHI. The user group of the misuser in this type of threat is not important. The motivation of the misuser and the technical or other means that he/she employs to commit the misuse are the factors that determine the risk level and the extent of damage. For instance a student who has sufficient computer skills and a strong urge to prove himself can cause much more damage than a faculty member who does not have enough technical capabilities.

Threat 4 type misuses are committed by physical intruders. The misuser in this type of threat does not have any access rights as such but somehow gains physical access to the organisation that manages e-PHI. For example a theft of hardware or e-PHI by outsiders will constitute a Threat 4 type misuse. Such physical intrusions by unauthorised outsiders can result in serious compromise of confidentiality, integrity and availability.

Threat 5 type misuses are purely technical threats where attack is mounted on the information system from a remote place. Here the misuser does not even have the physical access to the organisation's premises. Denial-of-service attacks are an example of Threat 5 type threat that threatens availability of e-PHI. The risk of Threat 5 type misuses is related to the external connectivity of the information system to the publicly accessible networks. Greater connectivity will lead to greater danger of the system being exposed to the Threat 5 type misuses. Our hypothetical dental information system exchanges e-PHI with other organisations so each of the those links can serve as access points by misusers.

Motive of an attack is an important characteristic that defines a threat. For Threat 1 type it is accidental so there would be no motive. However for the rest of the threat categories, it is important to taxonomise the motives. [8] presents a taxonomy of threat motives that can motivate Threat 2 to Threat 5 type misuses shown in Figure 4.3.

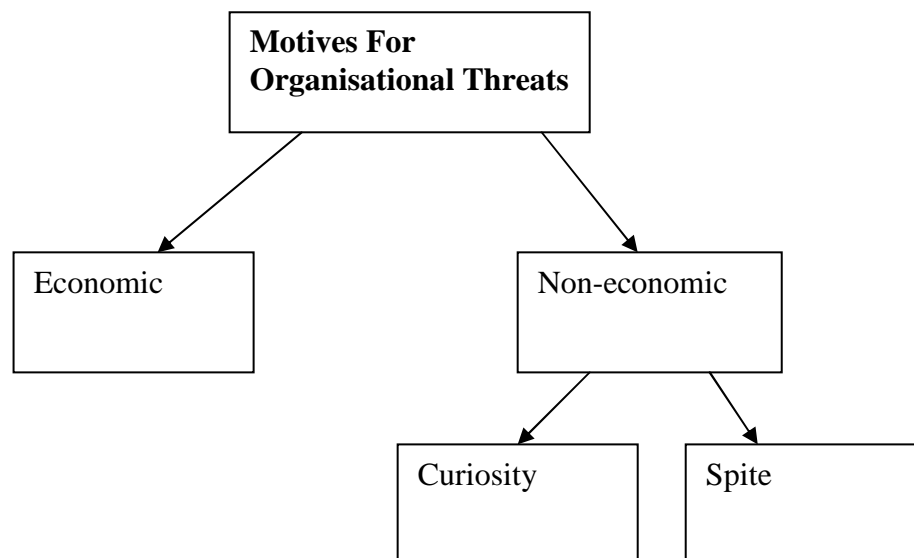


Figure 4.3: Taxonomy of motives for organisational threats



Firstly there is a separation between economic and non-economic motives. Stealing e-PHI for profit is an economic motive. In a dental school context the e-PHI concerning the dental health of a patient can be of monetary value to a dental insurance company. In the non-economic category there are curiosity and spite. Users who has access rights to e-PHI are subject to curiosity. For example a receptionist may be tempted to look up the contact details of a celebrity. The other non-economic motive is spite where the misuser wants to inflict harm to see others suffer as a result. A disgruntled ex-employee of a dental school who mounts a denial-of-service attack is motivated by spite.

#### 4.1.2 Systemic Threats

As mentioned previously systemic threats for e-PHI arise from the many flows of e-PHI among the various health care entities. Figure 4.4 demonstrates a hypothetical scenario of Alice's e-PHI flow through the health care industry adopted from [8].

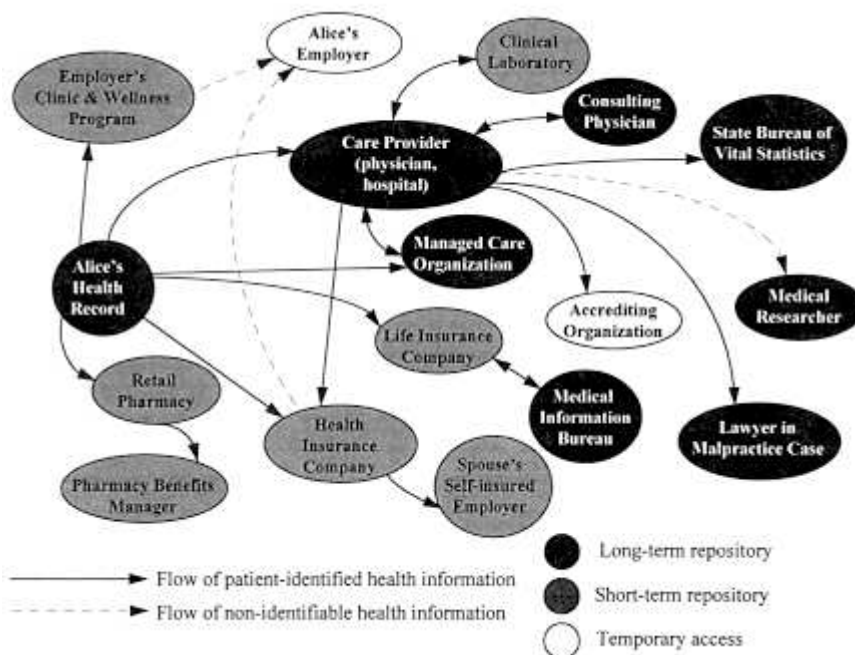


Figure 4.4: Flow of e-PHI through the health care industry (reproduced from [8])

Figure 4.4 shows that there are various types of organisations that access and store e-PHI. This means that e-PHI of a patient can end up with any number of organisations. The lack of uniformity in the organisational security policy and perception can lead to

serious weak links in the systemic flow of e-PHI. Systemic concerns about the privacy of patient-specific health information are generally rooted in the use of such information in a manner that acts against the interests of the individual patient involved [8]. Such systemic threats can cause serious breach of patient privacy and there are already reported cases of discrimination based on e-PHI for employment and insurance eligibility.

In Figure 4.4, each organisation needs access to Alice's e-PHI for specific purposes. For example, care providers need it for assessing her medical needs and developing treatment plans etc. Health insurance companies need it for processing insurance claims. Clinical laboratories need it for conducting appropriate diagnostic tests. Each organisation will have some form of organisational policy regarding security of e-PHI. However between different groups of organisations there is no consensus of policies. For example a health insurance company's definition of legitimate access is likely to be different from a physician's.

Here is a scenario of a hypothetical systemic threat taken from [8]. Let's consider the interaction between Alice's physician and her health insurance company. Alice consented to collection of her e-PHI for provision of health care. However when her physician sends her e-PHI to her health insurance company for claims processing, the insurance company uses her health details for assessing future insurance eligibility. This use of her e-PHI was not intended by Alice and is not in her interests. It has occurred because of the organisational policy of the insurance company that did not prohibit such use.

Another example of a systemic threat is where her physician discloses Alice's e-PHI to a malpractice lawyer because of a lawsuit in debate. The lawyer firm does not maintain the same standard of security controls as the physician and as a result Alice's e-PHI gets disclosed to a seller in the black market. Potential employers access her e-PHI from the black market and makes employment related decisions based on her e-PHI.

It can be seen that once the information leaves the hands of the health care provider, and it is stored off-site with the secondary user, that information is at the discretion of that secondary user site.

## 4.2 Countermeasures

In this section we discuss the countermeasures proposed by the US National Research Council for its threat taxonomy.

Table 4.1: Summary of countermeasures for organisational threats (adapted from [8])

Type	Threat	Countermeasure
1	Mistake	Organizational and simple technical mechanisms
2	Improper use of access privileges	Organizational and technical mechanisms such as authentication and auditing
3	Unauthorized use for spite or profit	Organizational and technical mechanisms such as authentication and auditing
4	Unauthorized physical intrusion	Physical security and technical mechanisms such as authentication and access controls
5	Technical break-in	Technical mechanisms such as authentication, access controls, and cryptography

Table 4.1 summarises the countermeasures proposed for each type of threat. For Threat 1 type threats, simple, administrative mechanisms to deter the breach are considered to be more effective than the sophisticated technical measures [8].

For Threat 2 type threats deterrence is the main countermeasure. Education of staff, appeals to ethics and strict sanction policy are administrative deterrence measures. Technical deterrence mainly consists of keeping of detailed audit trail and detection through analysis of the audit data. Obstacle-based technical mechanisms can also play a role. Strong authentication and encryption can make the job of the misuser more difficult.

For Threat 3 type threats using a combination of obstacles and deterrence is effective. Reasonable obstacles should be chosen so that they do not interfere with authorised use and at the same time prevent unauthorized access. The deterrence steps used against Threat 2 can be applied in the same manner. In particular audit trails are effective at deterring this type of threat.

For Threat 4 type threats physical security measures are the essential. Additionally technical means can be used to complement the physical protection. Technical security measures such as strong authentication, access control and audit control can be used as

both obstacles and deterrence.

For Threat 5 type threats the countermeasures are based purely on the obstacle approach. Deterrence mechanisms generally do not work well against determined outsiders. Strong authentication and access control can be used.

Systemic threats are difficult to counter using only the features of the information system. The US National Research Council argues that technological safeguards play almost no role in controlling secondary use of patient information (i.e. use by nonprovider parties) [8]. It further argues that industry-wide standards or regulations that support uniformity in the security policies and implementation of the health care organisations need to be developed and adopted for mitigation of systemic threats.

Let's consider the first hypothetical scenario of system threat given in Section 4.1.2. When Alice's e-PHI leaves the hands of her care provider it is stored with a secondary user, namely the health insurance company. Once the information is stored with the insurance company, access to Alice's e-PHI is at the discretion of that secondary user site. Therefore no amount of technological controls implemented at the care provider side will secure Alice's e-PHI. Thus from this analysis it can be seen that the mitigation of systemic threats require countermeasures at the level of public policy that will reduce the gaps between organisational security policies of the individual health care entities.

We compared the security controls specified in the HIPAA Technical Safeguards against the countermeasures shown in Table 4.1. From our comparison we found some similarities as well as differences between the HIPAA standards and the countermeasures. Authentication, access control and auditing can be found in both sets of security measures. On the other hand, Transmission Security and Integrity measures which are found in HIPAA are not present in the set of countermeasures from the US National Research Council. Apart from authentication, access control and auditing, the only other technical security control shown in Table 4.1 is cryptography. Use of cryptography can be used for implementing some Transmission Security and Integrity controls such as encryption but it is not clear from [8] if that is the intended use of cryptography. Thus we argue that the standards in the HIPAA Technical Safeguards offer a more fine-grained classification of the technical

controls to protect e-PHI.

### 4.3 Discussion

In this chapter we presented an existing taxonomy of threats against e-PHI and countermeasures for them. We explained the difference between organisational and system threats as specified in [8]. We put the different types of threats into the context of our dental information system to explain the taxonomy.

We examined the countermeasures for the threats proposed by [8]. From our analysis we verified the claim made by the US National Research Council that technical countermeasures on their own, are not sufficient for mitigating systemic threats.

We found some differences and similarities between the HIPAA standards and the set of technical countermeasures proposed in [8]. We found that Transmission Security and Integrity controls which are included as standards in the Technical Safeguards of HIPAA are not present in the set of countermeasures found in [8]. Instead encryption is included as another technical countermeasure in the the US National Research Council's taxonomy of countermeasures. We argue that HIPAA's classification is more fine-grained since Transmission Security and Integrity species more detailed security mechanisms compared to encryption which can be used to implement either of the two. The US National Research Council's countermeasures were published in 1997 and the final HIPAA Security Rule was published in the US Federal Register in 2003. We suspect that the countermeasures identified in [8] were used as a source in drafting of HIPAA although we cannot verify our speculation at this stage.

# 5

## Our Survey Methodology

In this chapter we describe and justify our survey methodology for our objective of eliciting security requirements for dental information systems from the US dental schools. In Section 5.1 we discuss the purpose of our data collection and analysis. Section 5.2 outlines the constraints of our investigation that affected our choice of data collection method. In Section 5.3 we discuss the alternative data collection methods and justify our decision to use a survey. In Section 5.4 we describe our survey instrument and provide justifications for our design decisions. In Section 5.5 we discuss the survey administration process followed by discussion of sampling method in Section 5.6. In Section 5.7 and Section 5.8 we discuss the response rate for our survey and data analysis techniques we used respectively.

## 5.1 Data Collection Requirements

Our research objective was to focus on a small subset of CEs under HIPAA, namely US dental schools and study their perceptions about security requirements for their e-PHI. The purpose of our data collection was to gather information from the US dental schools regarding their understanding of the HIPAA security requirements for their enterprise dental information systems.

Our review of the literature in Chapter 3 identified threat modeling as an effective way of eliciting security requirements. We pointed out that specific works on security threats mostly advocate the approach where it is left up to the security engineer to enumerate the security threats and no data is collected from the users. However our main research objective dictated data to be collected from US dental schools.

There were two specific goals that we set out to achieve from our experimentation. Our first goal was to find out about the general perception about the HIPAA provisions and e-PHI security held by the US dental schools. The second goal was to elicit specific security threats to e-PHI that they are concerned about with regard to HIPAA.

For the first goal, we needed some data that reflects the US dental schools' perception about HIPAA and security of their e-PHI. For this, both quantitative and qualitative data was required. For the second goal of eliciting security threats we mostly needed qualitative data that describe scenarios of security threats.

## 5.2 Constraints

There were two main constraints in our data collection which affected various aspects of our methodology. Firstly there were time constraints. Being only a master's level research we had one year time frame for the entire investigation. This meant that we had to complete data collection and analysis at least in 9 months to allow for writing up of the results.

Secondly there were geographical constraints. We were based in New Zealand dealing

with the dental schools in the United States. Therefore it was not possible to directly interact with the participants of our study.

## 5.3 Alternative Methods Of Data Collection

We evaluated the requirement elicitation techniques that involve the users discussed in Section 3.1.5 for our study.

Surveys are just one of the communication method that can be used for requirement elicitation. Their main advantage is that they are effective when there is a need to reach many research subjects [26]. The more direct forms of interaction such as interviews and group workshops are generally considered to allow more in-depth analysis of fewer subjects. However these methods require direct contact time with the research participants. Thus given our geographical constraint, they were not feasible.

Prototyping is well-suited for getting feedback on some first-cut implementation of some functional requirements. In our case we need data related to perception about security threats and it is awkward to create a prototype of security threats. Thus prototyping was not chosen.

Specialised techniques such as protocol analysis and discourse analysis are designed to improve the inherent limitations of the traditional techniques such as surveys and interviews. However they require significantly more contact time with each research subject. So despite their advantages, our time and geographic constraints prevented these techniques from being used in our study.

Our evaluation resulted in the conclusion that a survey-based data collection would be the most suitable data collection method for our study.

## 5.4 Survey Instrument

We had a co-researcher based in the US who collaborated with us. Dr Gary Guest who is the dean of clinical administration at the University of Texas dental school helped us



with the design of survey instrument. He reviewed the questions and offered suggestions as to how we could make them more effective. A breakdown of sections in our survey instrument is provided in the following list.

1. General
2. Access Control
3. Transmission Security
4. Audit Control
5. Integrity
6. Entity Authentication

The survey was structured according to the standards in the Technical Safeguards of the HIPAA Security Rule. Please refer back to Section 2.2 for detailed discussion of the standards. It can be seen that for each standard there is a corresponding section in our survey instrument.

For our first goal of finding out about the general perception of the participants we designed five general questions that were not limited to any particular standard. These questions belonged to the General section which is the first item on the above list. They did not follow any particular pattern. An example of the general question was “Please number each standard in the order of your concern level from 1 to 5 (5 being the most concerned to 1 being not concerned at all)”. The response format required for the general questions varied. Structured as well as unstructured response formats were required for the general questions. General questions were placed first to give the respondents a chance to become familiar with the whole survey and be ready to answer the more specific questions about each standard. Among the general questions ones that required structured responses were presented first to give a sense of easiness to the starting respondents.

After the general questions there were two types of questions that followed set patterns. These questions were designed to gather information about the security threats that the

participants were concerned about for complying with HIPAA. We refer to these questions as type-1 and type-2 questions. For each HIPAA standard we asked these type-1 and type-2 questions. We show examples of these questions for the Audit Control standard in the following list.

1. Type-1 “Are you satisfied with your current information system with respect to Audit Control? If not, please describe why”
2. Type-2 “Please describe a scenario of system use that you perceive as non-HIPAA compliant with regard to Audit Control”

The type-1 and type-2 questions were aimed to discover threat scenarios that the dental schools were concerned about. The two types of questions were phrased differently to get the respondents to think in two different ways. With type-1 questions, we do not explicitly ask for description of scenarios but we try to get the respondents to think about their current system. If a respondent is not satisfied with security status of his/her organisation’s current information system, he/she is asked to describe the reason.

With the type-2 questions we explicitly ask for description of threat scenarios. The word threat was originally included in the question but later omitted because in the process of obtaining ethics approval we were asked to remove the word threat. So we replaced the term ‘threat scenario’ with the phrase ‘scenario of system use that you perceive as non-HIPAA compliant’. An example threat scenario was included in the survey so that the respondents had a clear idea as to what to describe. For standards that have implementation specifications defined for them such as Access Control, the two types of questions were asked for each implementation specification.

The type-1 and type-2 questions mostly required unstructured responses. Questions that require structured responses have the advantage that they are easy to be answered by the respondents but they fail to capture all that is in the respondents’ minds. Also there is the danger that by providing choices we influence the respondents’ perceptions in an unwanted manner. We were conscious of the issue that it might affect the response

rate. However, we saw little merit in getting a series of multi-choice responses for serving our purpose of eliciting security requirements.

Apart from the type-1 and type-2 questions, we designed some questions that were unique to a particular standard. These questions did not follow any set patterns. For example for Audit Control, we asked the following question.

“Do you think dental information systems need to maintain an application-level log of user activities that is separate from database and OS level logs?”

These questions were customised to each HIPAA standard to gather specific user perceptions about the standard. For these questions we used a combination of structured and unstructured response formats.

For all our structured response questions where respondents had to make choices, we included ‘no response’ options. Not including such options forces the respondent to give a response but we did not want to distort the responses of individuals who genuinely have no opinion. Since we could not assume that everyone has a clear opinion towards our questions, we decided not to include any questions that force choice.

Our survey instrument consisted of twenty six questions in total. For the complete listing of survey questions, please refer to Appendix A.

## 5.5 Survey Administration

It has to be noted that no pretest was conducted for our survey. Time constraint prevented us from conducting a pretest. Although it is a limitation of our methodology, to our knowledge this study is the first of its kind and is intended to serve only as an exploratory study. We expect that future studies of similar kind can use our survey methodology as the pretest on which to improve.

Once our questions were finalised, the survey instrument and its administration procedures was subject to ethics approval from the University of Auckland. We obtained ethics approval under the following conditions.

1. We preserve confidentiality throughout the research process.

2. We make aggregate results available to participants on request.
3. We store information gathered for a period of six years for possible further work. After that period destroy the information by electronically deleting them from the media in which the information was stored.
4. We give to participants the right to withdraw from the project at any time. Also give them the right to withdraw their information/data up to 15 Dec 2005.
5. Present Participation Information Sheet to respondents outlining the terms and conditions of taking part in our research as listed above.
6. Obtain explicit consent from the respondents by asking them to read the Consent Form.

The Participant Information Sheet and the Participant Consent Form can be found in Appendix B

Once we obtained ethics approval to conduct our survey, Dr Guest helped us extensively with the administration of the survey instrument. One of his technical staff was able to design a secure website through which the participants were to complete the survey.

The online survey was made up of three pages as shown in Figure 5.1, Figure 5.2 and Figure 5.3.

The first page of the survey website was the participant information sheet which gave the respondents the background of the research and explained the terms and conditions of taking part in the research. We provided a link that read 'Continue' at the bottom of the first page to confirm that they read the page and they are willing to proceed to the second page. The second page was the participant consent form where they had to finally consent to taking part in the study. The respondents had to click on the 'I Agree' link at the bottom of the consent form to proceed to the third page that contained the actual survey questions.

Once the design of the website for our online survey was finalised, Dr Guest sent invitation emails to every dental school in the US through the American Dental Education



## Participant Information Sheet



**Title :** An Investigation of HIPAA Security Requirements for the US dental schools

**Researchers :** Professor Clark Thornborson / Jinho Lee / Dr Gary Guest

This research is being undertaken as part of a ME(Master of Engineering) thesis work at the school of engineering by Jinho Lee at the University of Auckland, NZ in collaboration with Dr Gary Guest at the University of Texas Health Science Center at San Antonio Dental School. There are varying interpretations of the HIPAA security rules among different health providers. The provisions have been written in a very general and broad manner deliberately to ensure high applicability. This research aims to investigate such interpretations among the dental schools in the USA. It is hoped that the results of this research will allow better security requirements to be specified for dental IT systems. Also it is expected to broaden the understanding of security issues relating to patient information and then provide some technical recommendations.

Our research involves the distribution of a questionnaire to gather dental schools' understanding of the relevant provisions. Dr Guest, as a member of the ADEA section for Dental Informatics, kindly offered to use his access to the ADEA listserv in identifying potential respondents. Through this listserv your organization has been selected as a potential participant.

Confidentiality will be preserved throughout the research process. If the information you provide is reported or published, this will be done in a way that does not identify you as its source.

Aggregate results will be made available to participants. Also participants will be allowed to request access to preliminary results via Dr Guest. Consent form will have his email address so should you wish to request such access, you can do so.

The information you provide will be stored for a period of six years for the purpose of possible further research. After that period the information will be destroyed by electronically deleting them from the media in which the information was stored.

Please note that as a participant you have the right to withdraw from the project at any time. Also you have the right to withdraw your information/data up to 15 Dec 2005.

This research is funded by New Economy Research Fund of New Zealand, contract UOAX0214, "Software techniques and systems for the protection of intellectual property".

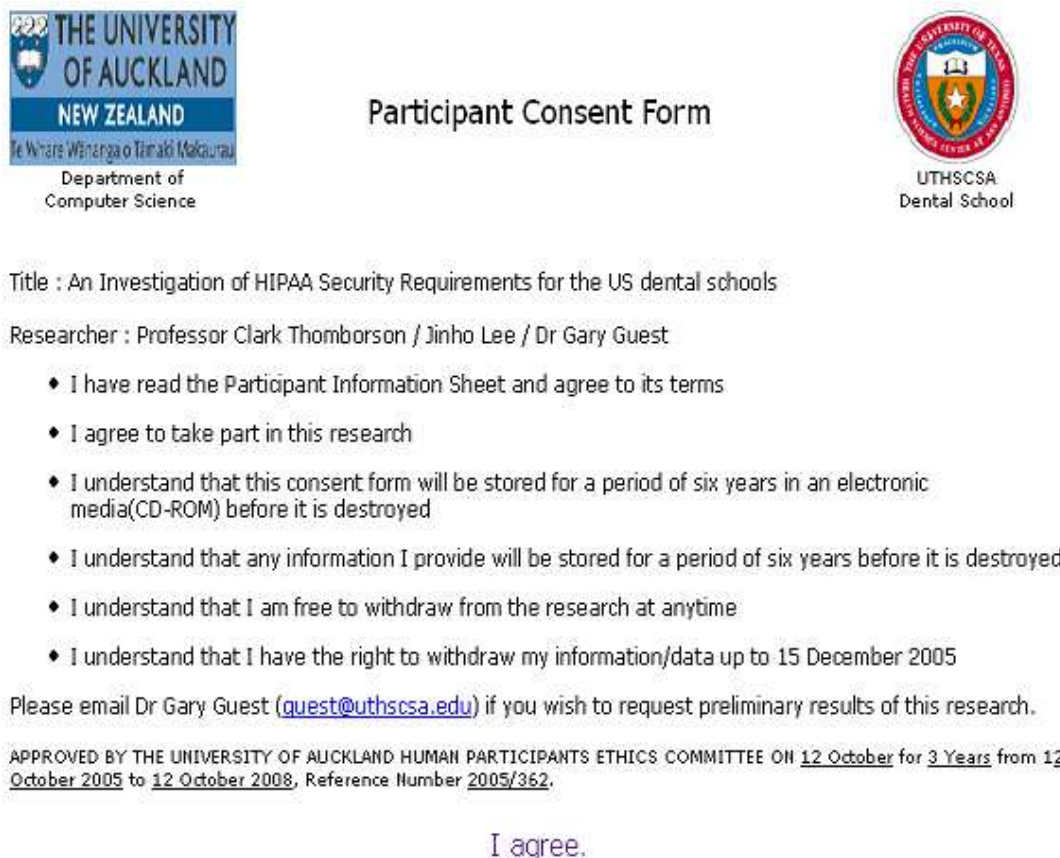
It is anticipated that participation in the questionnaire will take no more than one hour.

### Contacts

Professor Alan Williamson (Head of Department)  
+64 (9) 373-7599 ext87922, ag.[williamson@auckland.ac.nz](mailto:williamson@auckland.ac.nz)


Figure 5.1: First page of the online survey - Participant Information Sheet

Association(ADEA). The emails were addressed to the respective deans of the dental schools. The email explained the purpose of the study and asked for participation of the recipient's organisation. It also asked the deans to forward the letter to the appropriate personnel within the organisation to complete the survey. We requested that the survey be completed by the person in the organisation who is responsible for HIPAA compliance, or else by someone who is aware of the security issues regarding their e-PHI. We specified an initial deadline of one month from the date of the invitation letters. After this initial deadline we received four responses. Dr Guest oversaw the collation and anonymisation of the data. While we started our analysis of the data, to get some more responses Dr Guest sent a second invitation letter to the potential participants where he made a more personal appeal. We suspected that the cause for the low response rate was the nature of the survey questions that required narrative responses. Therefore in the second letter we asked them to just answer the questions that required structured responses if that was



**THE UNIVERSITY OF AUCKLAND**  
NEW ZEALAND  
Te Whare Wānanga o Tāmaki Makaurau  
Department of Computer Science

**Participant Consent Form**



UTHSCSA  
Dental School

Title : An Investigation of HIPAA Security Requirements for the US dental schools

Researcher : Professor Clark Thomborson / Jinho Lee / Dr Gary Guest

- ◆ I have read the Participant Information Sheet and agree to its terms
- ◆ I agree to take part in this research
- ◆ I understand that this consent form will be stored for a period of six years in an electronic media(CD-ROM) before it is destroyed
- ◆ I understand that any information I provide will be stored for a period of six years before it is destroyed
- ◆ I understand that I am free to withdraw from the research at anytime
- ◆ I understand that I have the right to withdraw my information/data up to 15 December 2005

Please email Dr Gary Guest ([quest@uthscsa.edu](mailto:quest@uthscsa.edu)) if you wish to request preliminary results of this research.

APPROVED BY THE UNIVERSITY OF AUCKLAND HUMAN PARTICIPANTS ETHICS COMMITTEE ON 12 October for 3 Years from 12 October 2005 to 12 October 2008, Reference Number 2005/362.


I agree.

Figure 5.2: Second page of the online survey - Participant Consent Form

putting them off. From the second iteration, we received three more responses.

Apart from the reminders with personal appeals we took other measures in the survey administration process to maximise the response rate for our survey. Firstly we emphasised that this research is being undertaken at highly regarded universities. So we made it clear to the potential respondents in our invitation email that this is a joint investigation between the University of Auckland and the University of Texas. We thought that having a US-based university collaborating with us will improve the respondents' credibility in us as researchers. All three pages of our website displayed the respective logos of the two universities. Also for the same purpose of establishing confidence, we sent the invitation emails via the ADEA email list to which Dr Guest had access.


Secondly we assured the respondents that confidentiality of their participation will be preserved. This was actually part of the University of Auckland ethics approval requirement. So on the participation information sheet and the consent form, we specified details



**THE UNIVERSITY OF AUCKLAND**  
NEW ZEALAND  
Te Whare Wānanga Tāmaki Makaurau

Department of  
Computer Science

## HIPAA's Security Requirements



UTHOCCA  
Dental School

There are varying interpretations of the HIPAA's security rules by different providers.

This survey is intended to gather useful information about such interpretations thereby allowing better security requirements to be allocated for the health IT systems.

If your organization has conducted some form of risk analysis previously, please provide us with the results as this would be extremely helpful to our research. We intend to publish the aggregate survey results to the dental school listserv. Please note that the results publisher will preserve anonymity.

**Respondent Details (\*required)**

Institution\*

Role\*

**Technical Safeguards**

General

1. Please number each area of the HIPAA can give me listed below in order of your level of concern in terms of existing system compliance.  
(5 for Very Concerned and requires immediate attention to 1 for Not concerned at all)

- Access Control (access policy, user id etc)  
 1  2  3  4  5  no response
- Transmission Security (electronic transmission of patient data eg email)  
 1  2  3  4  5  no response
- Audit Control (recording user activities for detection of security breach)  
 1  2  3  4  5  no response
- Data Integrity (making sure data is not altered or destroyed in unauthorized way)  
 1  2  3  4  5  no response
- Entity Authentication (verifying that an entity seeking access to patient health information is actually the one claimed to be doing so)  
 1  2  3  4  5  no response

2. Do you think your organization has security issues in the way of patient care? (if yes, please explain briefly.)  
 yes  no  no response

Figure 5.3: Third page of the online survey - Survey Questions

such as for how long the data will be kept. We expected that this would prevent potential respondents from not taking part because of concerns about confidentiality.

Thirdly we made an offer to provide the final results of the survey in the form of aggregate data. By providing a potential reward, we expected greater response rate.

## 5.6 Sampling

Our target population was the US dental schools. Since we were dealing with a small population which consisted of fifty six dental schools invitations were sent to the entire population. In our invitation email, we explained the motivation and the content of the survey. Then we asked the survey be answered by a suitable personnel within the

organisation. Our goal was to get one response from someone at each dental school who is responsible for the HIPAA implementation or at least aware of the organisational perceptions about HIPAA security requirements.

## 5.7 Response Rate

Despite our measures to increase the response rate, we received seven responses after the final deadline for survey participation. This was out of the fifty six potential respondents therefore the response rate for our survey was 12.5%. The low response rate means that our data is not representative of the target population. Nevertheless it was still possible to analyse the data we received to identify hypotheses for future works since this was an exploratory study. In particular, the unstructured, open-ended responses allowed qualitative analysis that did not require much in terms of statistical significance.

## 5.8 Data Analysis Techniques

In our analysis of the survey responses we used the following techniques.

Statistical Analysis Techniques - Despite the low response rate we applied some statistical methods to analyse our data. We used Student's t-test to test some hypotheses about our observations of the survey responses.

Misuse Case Analysis - For the threat modeling technique we decided to use misuse case analysis. We also considered the option of using attack trees. However following our comparative evaluation in Section 3.6 misuse cases were chosen as the better option for this particular study. Applying attack trees method on the initial threat model acquired from misuse case analysis would be a worthwhile effort but is outside the scope of this thesis. Narrative descriptions of threats by the respondents were modeled in terms of misuse cases. Diagrammatic notations for misuse case analysis were used in our analysis to represent threats and to see how the misuse cases interacted with the normal uses of the system.



Cluster Analysis - We tried to categorise each misuse case identified from the survey responses into the existing taxonomy of threats to e-PHI discussed in Chapter 4. Through this analysis we examined if the existing taxonomy needs to be improved in any way.

## 5.9 Discussion

In this chapter we described our survey methodology. We also outlined our design decisions which affected various parts of our methodology.

Design of our research methodology was driven by our main research objectives, findings from our literature review and our constraints. For our goal of eliciting user security requirements from the US dental schools, we chose to elicit the security threats which the schools are concerned about. Our decision to elicit security threats was based on our review of literature in Chapter 3. Our need to get information from the users and our constraints discussed in Section 5.2 meant that a survey-based methodology would be the most suitable option.

We described and justified the design of our survey instrument. A notable characteristic of our survey instrument was that it contained many open-ended questions. This was especially true for questions that aimed to elicit security threats that the respondents were concerned about. We deliberately designed the survey questions this way so that the respondents freely describe the threats that they perceive to be important. We did this despite the common belief that the number of open-ended questions should be minimised in a survey. The reason for our decision was that we did not want to unduly influence the respondents' perceptions by giving them options that we came up with.

We described and justified the administration of our survey instrument. Our survey methodology was subject to ethics approval from the University of Auckland. One major limitation of our survey-based methodology was that it did not involve a pretest. Time requirements for obtaining prevented us from conducting a pretest. Online survey was chosen as the way to administer our survey instrument because it seemed to be the best way to attract responses given our geographical constraint. Despite our efforts to increase

---

response rate, the response rate for our survey was low at 12.5%. We speculate that the open-ended nature of our survey might have contributed to the low response rate. Possibly another survey that contains mostly structured response questions can be administered to the same target respondents to see if it results in better response rate. However, it is outside the scope of this thesis.

We outlined data analysis techniques that were used to analyse the responses. Some statistical methods were used on the structured responses to find some significant user perceptions despite our low response rate. Qualitative analysis techniques including misuse case analysis and cluster analysis were used on the narrative, unstructured responses to elicit and analyse the security threats that our respondents are concerned about.



# 6

## Results and Discussion

In this chapter we present the findings from our survey. In Section 6.1 we discuss our survey respondents. In Section 6.2 we present and analyse our general findings. Between Section 6.3 and Section 6.12 we present our findings relating to the security threats identified from our survey. For complete listing of the raw data obtained from our survey, please refer to Appendix C.

### 6.1 Respondents

We identified three categories of respondents as shown in Table 6.1.

The majority of respondents were clinic administrators of the participating dental schools. There was one HIPAA officer and one CIO. Thus it can be seen from the titles of

Table 6.1: Survey Respondent Roles

Role	Frequency
Clinic Administrator	5
HIPAA Officer	1
CIO	1

the respondents that all of our respondents are in positions in their respective organisations which make them aware of the HIPAA and related security issues.

## 6.2 General Findings

From the responses to the general questions we discovered the following findings.

### 6.2.1 Areas of Concern

The respondents were asked to number each standard of the HIPAA technical safeguards according to their degree of concern from one to five. One meant that there is no concern whereas five meant the highest level of concern. In subsequent tables the names of the HIPAA standards are abbreviated as shown in the Table 6.2 for clarity.

Table 6.2: Abbreviations for the names of the HIPAA standards to be used in subsequent tables

Standard	Abbreviation
Access Control	AC
Transmission Security	TS
Audit Control	AU
Integrity	I
Entity Authentication	EA

Table 6.3 shows the responses to the question. Each row shows the responses from a given respondent. For clarity we abbreviated column titles so ‘R1’ refers to Respondent 1, ‘R2’ refers to Respondent 2 and so on.

For example, our first respondent R1 gave a rating of ‘2’ to Access Control, Transmission Security, and Integrity, indicating that these were of less concern than Audit Control and Entity Authentication. ‘nr’ stands for no response which means that our third respondent R3 did not specify a rating for Entity Authentication.

Table 6.3: Levels of concern for each HIPAA standard

	AC	TS	AU	I	EA	Mean(2 d.p.)	Var(2 d.p.)
R1	2	2	4	2	3	2.60	0.80
R2	3	4	4	3	3	3.40	0.30
R3	2	1	3	2	nr	2.00	0.67
R4	1	5	5	1	1	2.60	4.80
R5	2	3	2	2	2	2.20	0.20
R6	4	4	3	5	3	3.80	0.70
R7	1	1	2	2	2	1.60	0.30
Mean(2 d.p.)	2.14	2.86	3.29	2.43	2.33	N/A	N/A

The row means show that there are differences in the average levels of concern reported by our respondents. For example, R2 reported greater concern overall compared to R7. Also we computed sample variances for each respondent which are shown as row variances.

We aggregated the responses and calculated mean values for each standard which are shown as column means in the Table 6.3. Figure 6.1 provides a graphical representation of the the column means.

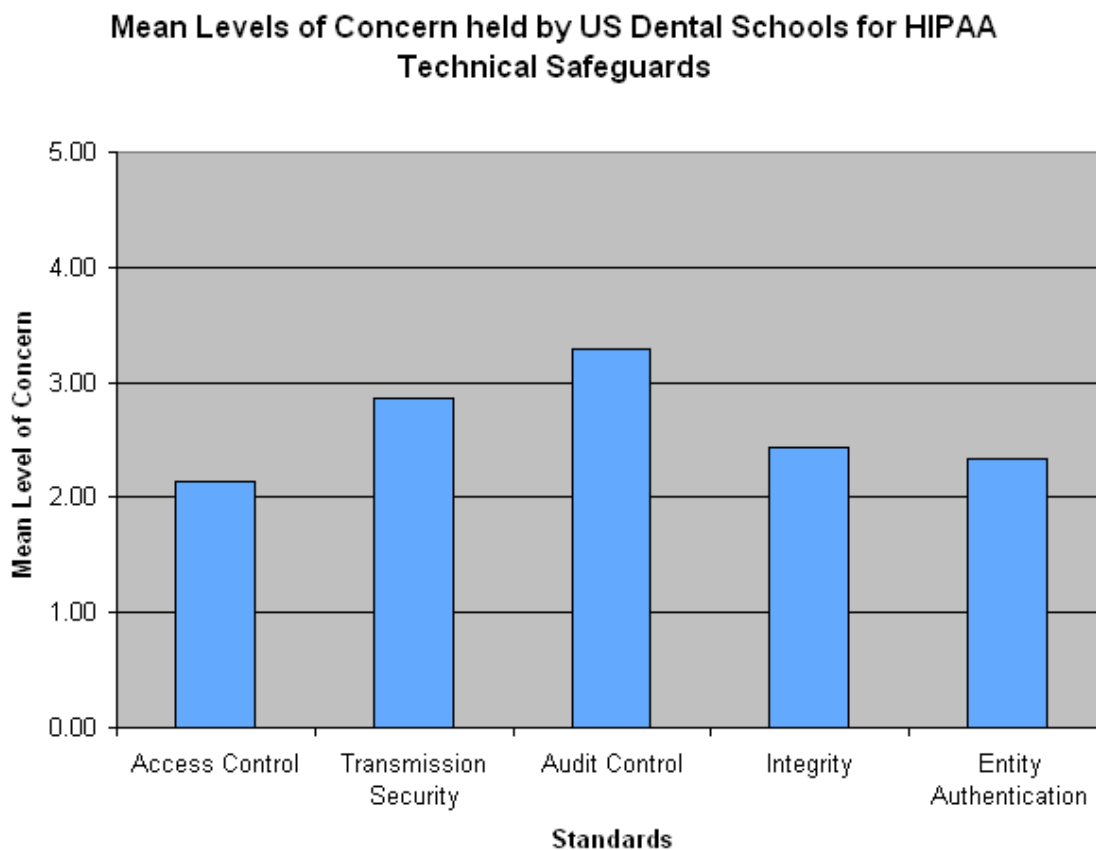


Figure 6.1: Audit Control had the highest mean level of concern.

Figure 6.1 shows that there are some differences between the mean values for each standard. For example, it indicates that Audit Control is the standard of HIPAA technical safeguards that our respondents were most concerned about followed by Transmission Security. To determine if these differences between the mean values are statistically significant, we performed Student's t-test for paired data. We compared the data for Audit Control against all the other standards. Table 6.4 shows the results of our t-tests. In all cases, the null hypothesis( $H_0$ ) was that the differences between the mean values are caused by chance.

$H_0$  : "The differences between the mean values for the level of concern are statistically insignificant and are caused by pure chance."

Table 6.4: Results of t-test between mean level of concern for audit control and the other standards

Standard	t-value	degrees of freedom	p( $H_0$ )
AC	1.92	6	0.103
TS	0.891	6	0.407
I	1.22	6	0.270
EA	1.87	6	0.111

Table 6.4 indicates that at the 90% confidence level we cannot not reject the null hypothesis for any of the four cases. However there were only seven respondents and the range of possible values was only five both of which severely limit the power of this statistical test [46]. We suspected a type-II error, of falsely retaining our null hypothesis.

My supervisor suggested I try the following statistical test based on the top choices of the respondents. In this test we have rescaled each respondent's rankings: 3 points for 'most important', 1 point for second most important, 0 for others. Where someone ranks two items equally, we assign fractional points as per the usual scoring in tournaments.

One benefit of this analysis, aside from its possibly greater statistical power, is that it gives equal weight to each of our respondents. By contrast, the mean values used in the t-test are highly affected by the responses of R4 and barely affected by the responses of R5, because the former had a much higher variance in their concern scores. For sample variances, please refer back to Table 6.3. The advantage of this rescaling is that it focusses the analysis on the most important standard, and it compensates for the greatly different

scales of our respondents.

Table 6.5: Rank ordered responses for the level of concern for each standard

Respondent	First	Second
1	AU	EA
2	AU, TS	AC, I, EA
3	AU	AC, I
4	AU, TS	AC, I, EA
5	TS	AC, AU, I, EA
6	I	AU, TS
7	AU, I, EA	AC, TS

Our lists of first and second most important concerns, by our respondents, are shown in Table 6.5. Note that three of the respondents gave more than one standard the same value as their first concern. Six of the respondents gave more than one standard the same value as their second concern. Based on the information in Table 6.5, we assigned points to each standard as specified. Table 6.6 shows the points for each standard under our point system.

Table 6.6: Points assigned to each standard

	AU	TS	I	EA	AC	Sum
R1	3	1	0	0	0	4
R2	1.5	1.5	0.33	0.33	0.33	4
R3	3	0	0.5	0	0.5	4
R4	1.5	1.5	0.33	0.33	0.33	4
R5	0.25	3	0.25	0.25	0.25	4
R6	0.5	0.5	3	0	0	4
R7	1	0.5	1	1	0.5	4
Sum	10.75	8	5.42	1.92	1.92	28
<b>Mean</b>	1.54	1.14	0.77	0.27	0.27	4
SSD	1.10	0.99	1.03	0.36	0.21	N/A

The mean values for the standards in Table 6.6 show that Audit Control has the highest mean value. Transmission Security has the second highest mean value followed by Integrity. Access Control and Entity Authentication had the same, lowest mean value.

We tested another null hypothesis too see if the differences in the mean values are statistically significant. Our new null hypothesis (Ho') was that the differences in the mean values under our rescaled point scheme are caused by pure chance. For this analysis



we used Student's t-test for paired data again. Similar to our first t-test Audit Control had the highest mean value so we compared the mean value for Audit Control with the rest.

Ho' : "The differences between the mean level of concern based on our point system are statistically insignificant and are caused by pure chance."

Table 6.7: Results of second t-tests between mean level of concern for audit control and the other standards based on our rescaled point system

Standard	t-value	degrees of freedom	p(Ho')
AC	3.02	6	0.023
TS	0.573	6	0.587
I	1.10	6	0.313
EA	2.61	6	0.040

Table 6.7 shows the results of our t-tests. It indicates that at the 95% confidence level, we can reject Ho' for Access Control and Entity Authentication. On the contrary we cannot reject Ho' for Transmission Security and Integrity.

We ran pair-wise tests for Transmission Security as well to see if it had any significant difference.

Table 6.8: Results of third t-tests between mean level of concern for Transmission Security and the other standards based on our rescaled point system

Standard	t-value	degrees of freedom	p(Ho')
AC	2.21	6	0.069
AU	0.573	6	0.587
I	0.580	6	0.583
EA	2.21	6	0.069

Table 6.8 indicates that at the 90% confidence level, we can reject Ho' for Access Control and Entity Authentication.

Therefore the results of our t-tests indicate that the respondents are not equally worried about every standard. We conclude at the 95% confidence level, that Audit Control is of greater concern to our respondents than Access Control and Entity Authentication. We also conclude at the 90% confidence level, that Transmission Security is of greater concern to our respondents than Access Control and Entity Authentication.

### 6.2.2 Perception about potential trade-off between security and patient care

We asked the respondents whether they thought e-PHI security could get in the way of patient care. The question was phrased as “Do you think your organization has security issues in the way of patient care? If yes, please explain briefly”. Responses to the question are shown in Table 6.9

Table 6.9: Responses to the question on potential trade-off between security and patient care

Respondent	Answer	If yes, why
1	Yes	logging activity
2	No	nr
3	No	nr
4	No	nr
5	No	nr
6	No	nr
7	No	nr

Almost all (six out of seven) of the respondents did not report tradeoff between security and patient care. One respondent indicated a trade-off with ‘logging activity’. We infer that respondent was referring to the slow response time of a dental information system that occurs when logging features are turned on.

## 6.3 Threat Model From The Survey Responses

In this section we present the findings that resulted from the type-1 and type-2 questions in our survey which were discussed in detail in Section 5.4. In those two types of questions we asked for narrative responses mainly describing reasons for any dissatisfaction with the current information system and scenarios of security threats respectively.

We have identified seven different misuse cases from the survey responses. Table 6.10 summarises the raw data on which the misuse cases were based. Corrections were made where a response was unclear, misspelled or ungrammatical. They are shown in square brackets in the table.

Table 6.10: Raw data from the survey describing the security threats and corresponding misuse cases

Misuse Case	Description in Survey Response
Password Sharing by Insiders	R1 - "password sharing"
	R1 - "concern for share of password, concern on who is also behind screen when system accessed remotely"
	R4 - "Students or Faculty sharing User ID / Password with peers"
	R3 - "An [authorized] person sharing their password with someone else. This is non-compliant with our Medical Center confidentiality agreement that is required annually to maintain [access] to our system. Such [non-compliance carries] significant internal penalties"
Data inconsistency resulting from multiple systems that are not integrated	R1 - "Having multiple clinic information systems that are not integrated causing inconsistent data"
	R1 - "eliminate shadow systems, have one CIS system establish who the patient is [and then] feed other systems"
	R6 - "Some academic departments maintain shadow databases that might not be secure"
Unauthorised Access Through Unattended Workstation	R4 - "Students logging on and then leaving the workstation unattended"
	R6 - "In some locations, the computer might be on longer than it should before logging off"
After-the-fact Modification of e-PHI for cover up	R4 - "A user attempting to modify the health record to hide an omission that led to an adverse outcome"
Theft of E-PHI stored in Desktop Computers	R5 - "Patient data kept on desk computers, rather than kept on the college server. [The] theft of a desktop computer caused notifying several hundreds of patients"
Disclosure of email used to communicate e-PHI	R6 - "Users sometimes send patient information in emails to outside people. I am not worried about emails being electronically intercepted, which is rare. I am worried that the recipient will not protect the email by leaving a [computer exposed]"
Clearinghouse breach that would draw us into investigation	R6 - "Clearinghouse could have [a] security breach that would draw us into investigation or lawsuit"

We used the semantics and notations of misuse cases for our threat analysis. Henceforth the term misuse case and threat will be used as synonyms. Figure 6.2 below shows all the misuse cases identified from the survey responses in misuse case notations.

There are two classes of misusers, namely inside misusers and outside misusers as discussed in Section 4.1. In Figure 6.2 the term misuser was used to represent both classes of misusers for simplicity of the figure. In the following sections we explain and analyse

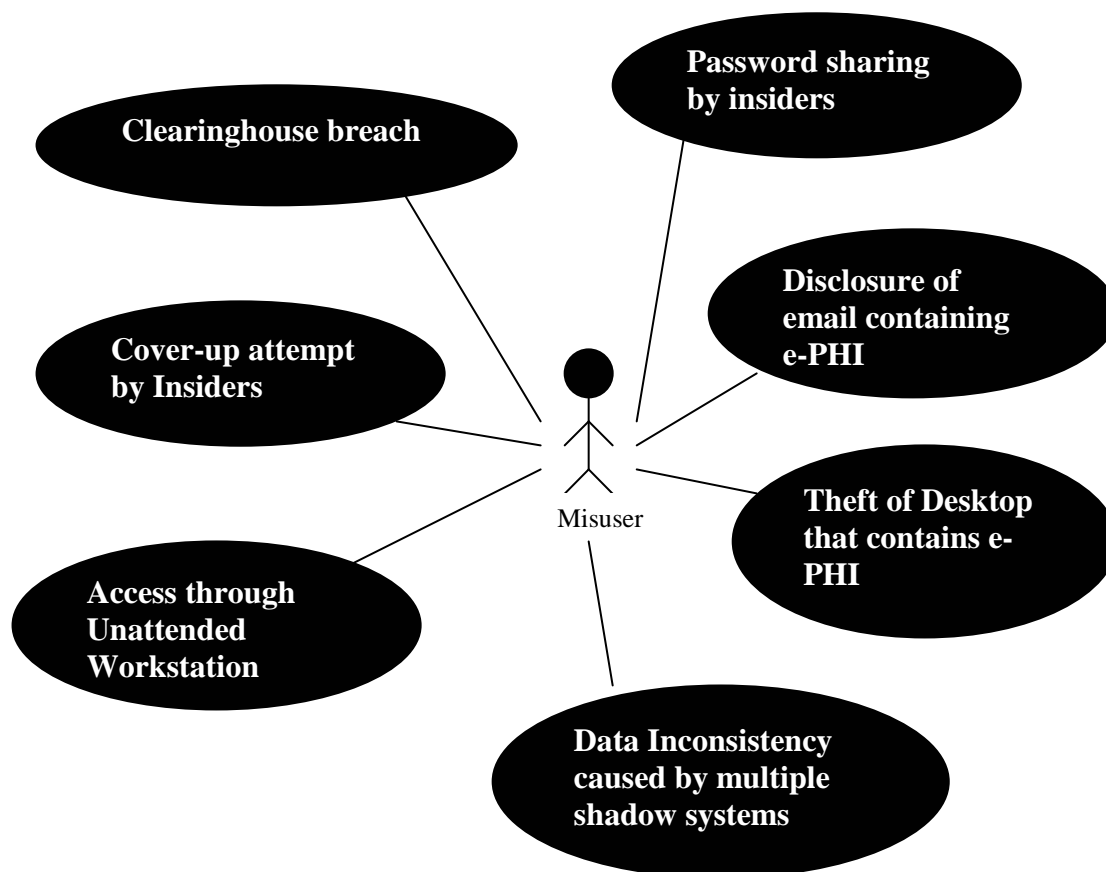


Figure 6.2: Overview of the misuse cases identified from the survey

the misuse cases in more detail. We examine how each misuse case can lead to violation of the three goals of e-PHI security discussed in Section 2.5.1. Then we classify each misuse case into the taxonomy described in Section 4.1. From this analysis we propose some improvements to the existing taxonomy. Finally we categorise the identified misuse cases into our improved threat taxonomy and analyse the types of threats that are causing concern for the respondents.

We note that many of the survey responses did not specify enough details to allow our analysis on their own. For example our first respondent, R1 specified “Password Sharing” as a security threat. However, the phrase “Password Sharing” on its own lacks information about the misuser and the specific misuse that can occur as the result of password sharing. In such cases, we made assumptions about what the respondents might have written, if they had described their threat more fully. Our assumptions were based on the system context for our enterprise dental information system outlined in Section 2.3.

## 6.4 Password Sharing by insiders

Password sharing by authorised insiders was identified as a security concern from the survey responses. Table 6.10 shows that three out of the seven respondents expressed concern about password sharing. Our first respondent, R1 identified it twice in his/her entire survey response.

The act of sharing one's password in itself does not violate any of the three security qualities for e-PHI. The asset in immediate danger is someone's password rather than someone's e-PHI. However, it often leads to other misuse cases where direct harm is done to e-PHI. An organisational threat occurs when the security policy of an organisation is violated. We assumed that security policies of health care organisations specify confidentiality, integrity and availability of e-PHI within their organisational boundaries as their security objectives. We argue that the act of sharing one's password constitutes an organisational threat because of the danger it poses to e-PHI. Please refer back to Section 4.1 for more detailed discussion of organisational threats.

Figure 6.3 and Figure 6.4 below show two hypothetical paths of misuse cases resulting from password sharing. We took students and faculty members as the misusers in our examples. Students are only allowed to access patients who are assigned to them by faculty members. Faculty members have access to more patient records and they have the task of signing off student works and assigning patients to appropriate students.

If a student password is shared, only the e-PHI of patients who are assigned to the student will be compromised. Another student might view or modify the e-PHI of patients not assigned to him using a borrowed password. This would lead to a security breach. If a faculty password is shared more serious breaches are possible. Faculty sign-off feature can be misused by someone who borrows the password of a unsuspecting faculty member. It can be a student or a peer faculty member who tries to sign off student works inappropriately. The access rights of a faculty member that allows patients to be assigned to students can be misused in the same manner. Students can end up with more patients assigned to them if a faculty password is being shared. Thus it can be seen that pass-

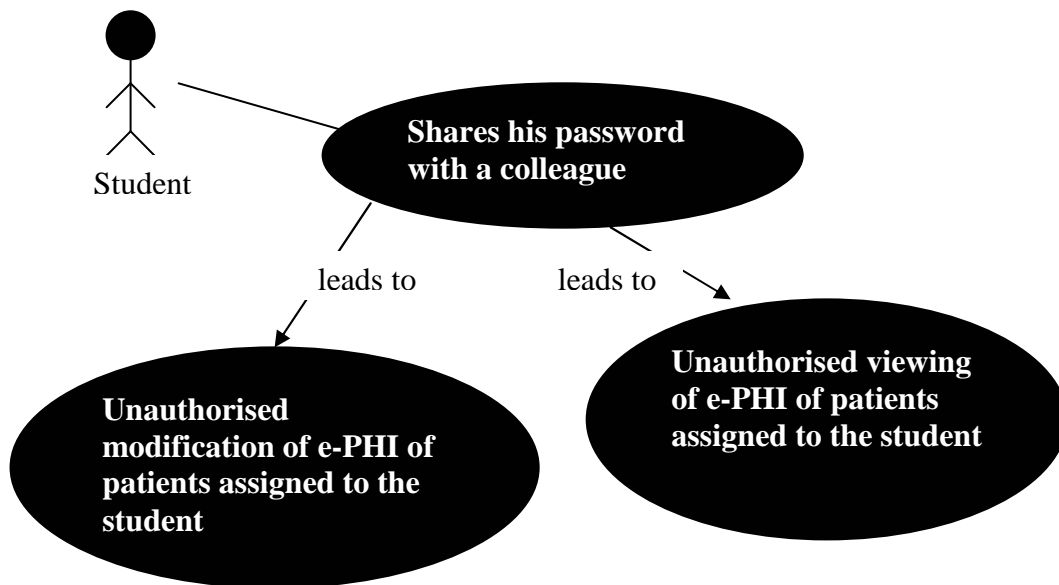


Figure 6.3: Misuse case where a student password is shared.

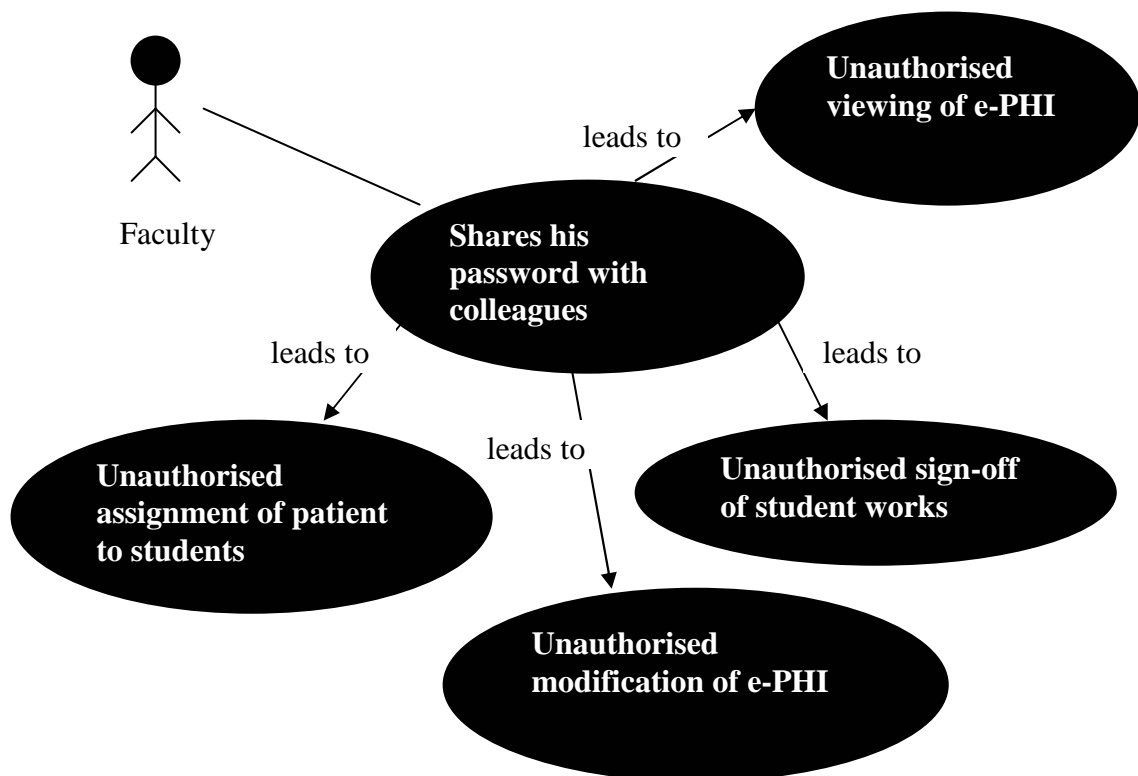


Figure 6.4: Misuse case where a faculty password is shared.

word sharing will lead to varying amount of risk depending on whose password is shared. Once a password is shared then there is no way to ensure confidentiality, integrity and availability of the e-PHI that the real owner of the password was allowed to access.

When a password is shared with another insider and the borrower accesses e-PHI in

unauthorised manner, the borrower is acting outside his/her access rights. Thus he/she is clearly committing a Threat 3 type misuse, of an insider going outside their access rights (see Section 4.1). The person who shares their password is also a misuser, but it is not immediately clear how to classify this misuse. In order to classify password sharing as a Threat 1 category (accidental misuse by insiders), there must be an accidental element in the breach of security. Voluntarily sharing one's password cannot be seen as accidental. Now let's consider the Threat 2 category of insiders abusing their access rights. In this category, the person who is committing the misuse is acting within the boundary of his/her access rights. The question is whether the misuser's normal access rights include the right to share his/her passwords with others. If the organisation does not forbid password sharing, then this act falls into the Threat 2 category. However, if one's access rights exclude the right to share the user passwords with others, it cannot be classified into the Threat 2 category.

In the latter case, password sharing is not in the Threat 3 category unless it is done for spite or profit. The misuse cases identified by our respondents do not mention motivation. We would presume that a faculty member who shares his/her password with a peer is unlikely to do so for spite or for profit. A naive insider who shares his/her password is clearly acting outside his/her access rights but he/she is not actually accessing the e-PHI. Thus most instances of password sharing will not fall into Threat 3. Threat 4 (unauthorised physical intrusion) and Threat 5 (unauthorised technical misuse) are only for unauthorised users so they are not applicable in this case. Thus we conclude that the threat of password sharing cannot be adequately categorised into the threat taxonomy presented in [8].

## 6.5 Physical Theft of Desktop Computers that Store e-PHI

One of the respondents, R5, identified physical theft of desktop computers that store e-PHI as a security concern. He/she reported a case of a physical theft of a desktop that contained e-PHI and having to notify hundreds of patients of the theft. Figure 6.5 demonstrates this misuse case being committed by a physical intruder and a malicious insider respectively.

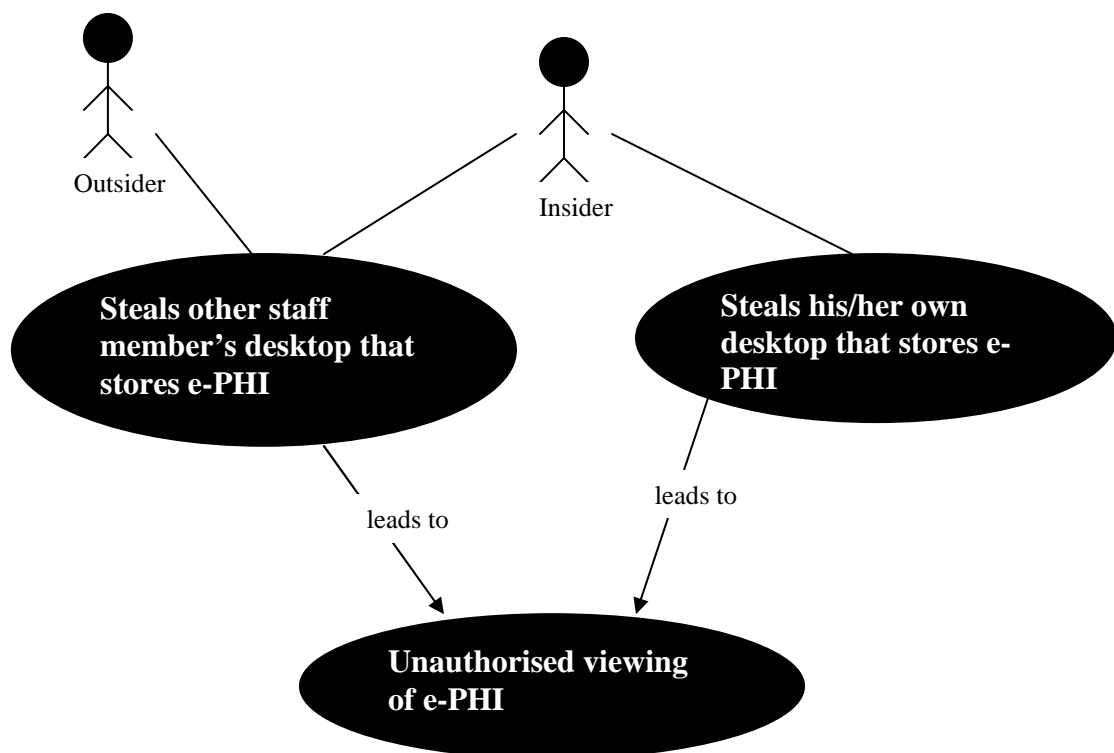


Figure 6.5: Misuse cases where a physical intruder or an insider steals desktops that stores e-PHI.

A physical theft of a desktop computer leads to a breach of confidentiality. If we assume that there is a secure central server, integrity and availability would not be affected so much because the e-PHI stored in the server is still secure. However without a central repository serious breach of integrity and availability can occur.

This misuse case is an organisational threat because internal or external misusers violate directly the security goals of the organisation. Let's firstly consider the case where an insider steals a desktop. We can exclude Threat 4 (Unauthorised physical intrusion)



and Threat 5 (Unauthorised technical misuse) type since they are outsider threats. The act of stealing a computer from his/her workplace cannot be seen as accidental. Thus it is not a Threat 1 (accidental misuse by insiders) type misuse. Also the misuser is clearly acting outside of his/her access rights when he/she decides to steal. So it is a Threat 3 (insiders acting outside their access rights) type misuse rather than a Threat 2 (insiders abusing their access rights) type. The respondent did not specify the motive of the theft. We presume that the motive of a theft is likely to be profit but it can also be curiosity or spite.

If a physical intruder breaks into organisational premises and steals a desktop, it is either Threat 4 or Threat 5 type misuse since an outsider is committing the misuse. We can classify it as a Threat 4 type misuse because the misuser gains access to e-PHI through physical means.

## 6.6 Cover-up attempts by Insiders

One of the respondents, R4, identified authorised insiders trying to hide omissions by inappropriately altering e-PHI as a security concern. Figure 6.6 demonstrates a misuse case where a dental clinician tries to cover up his/her mistake that led to an adverse outcome.

A dental clinician makes a diagnosis and provides some treatment accordingly. Then the patient suffers from severe side-effects because of a critical mistake by the clinician. So in order to avoid legal liability and embarrassment he/she decides to modify or even erase relevant part of the patient's e-PHI. As a consequence the patient can suffer unduly with no reparations. The security qualities of e-PHI in danger here are integrity and availability. Confidentiality is not a big issue since clinicians are authorised to view the e-PHI of their patients.

Dental malpractice lawsuits are increasing and thus there is ever more motivation for the dental clinicians to abuse their access rights for cover-up attempts. A real life example of cover-up attempt in health care domain can be found in [47] where a nurse was caught

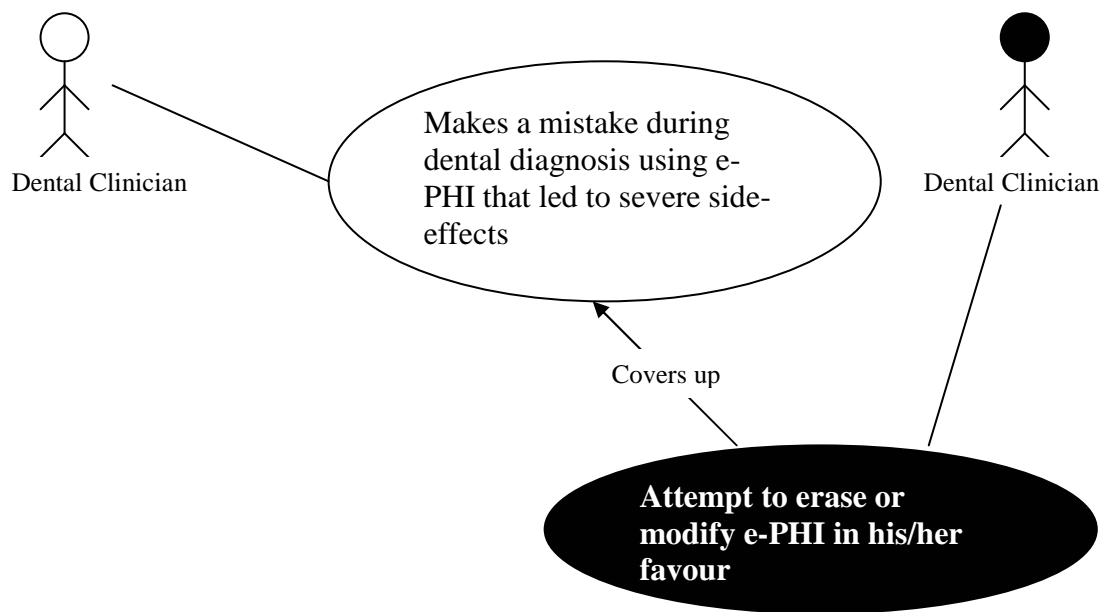


Figure 6.6: Cover-up attempt by a dental clinician to hide a malpractice.

for altering e-PHI after the death of a baby.

It is an organisational threat as it violates organisational policy directly. The misuser in this case is an authorised insider so we can safely exclude Threat 4 (unauthorised physical intruder) and Threat 5 (unauthorised technical misuse). Firstly there is element of intent in a cover-up attempt. So we cannot classify it as a Threat 1 (accidental misuse by insiders) type misuse. The deciding factor between Threat 2 (insiders abusing their access rights) and Threat 3 (insiders going outside their access rights) type misuses is whether the misuser is acting within or outside the boundary of his/her access rights. In this case because a clinician must have access rights to his/her patients' e-PHI to provide adequate care, he/she is abusing his/her access rights to commit the misuse. Therefore it can be classified as a Threat 2 type misuse.

However the motive of the misuser in this misuse case does not fit into the motive taxonomy presented in Section 4.1. Our survey response did not specify a motivation for this misuse case. We identified some potential motives for the misuse case and tried to classify them. Economic profit, spite and curiosity were the motives identified by [8]. Here the misuser is not committing the misuse because of economic reasons. There is no potential profit involved. Surely a malpractice lawsuit can cause financial burden

for a dentist but there are other factors such as desire to avoid humiliation and loss of reputation that might be motivating the misuser. Also the misuser is unlikely to alter e-PHI inappropriately for curiosity. Misuses motivated by curiosity mostly involve unauthorised viewing of e-PHI. Finally to hide an omission is not to hurt others so it is hard to argue that spite is the motive of the misuse case. Therefore the existing taxonomy of motives for misusing e-PHI does not handle the potential motives for this misuse case well.

## 6.7 Disclosure of emails that contain e-PHI

One of the respondents, R6, identified disclosure of emails that contain e-PHI as a security concern. This misuse case is when an insider sends emails that contain e-PHI and that email is read by someone other than the intended receiver. The respondent who expressed concern about email communication involving e-PHI said that he/she was not concerned about email being intercepted electronically as such. Rather the concern was more to do with careless keeping of the email on the recipient's side. Please refer to Table 6.10 for the actual response. As the respondent explicitly excluded more technical threats against email communication we will not concern ourselves with such threats in our threat analysis. The response implied that the concern is not the use of such emails itself but the improper management of those emails.

Figure 6.7 shows the misuse cases of two different types.

Disclosure of an email mainly violates confidentiality of e-PHI. Integrity and availability are less likely to be affected because emails usually only contain copies of e-PHI. A disclosure of an email that contains e-PHI can be both organisational and systemic threats depending on where the email was sent to. If unauthorised disclosure occurs within the organisation it would be classified as the former and vice versa. The organisational misuse can be further classified into Threat 1 (accidental misuse by insiders) or Threat 3 (insiders going outside their access rights). If the unauthorised disclosure of email was accidental it will be a Threat 1 type misuse. However if the misuser was actively looking for emails

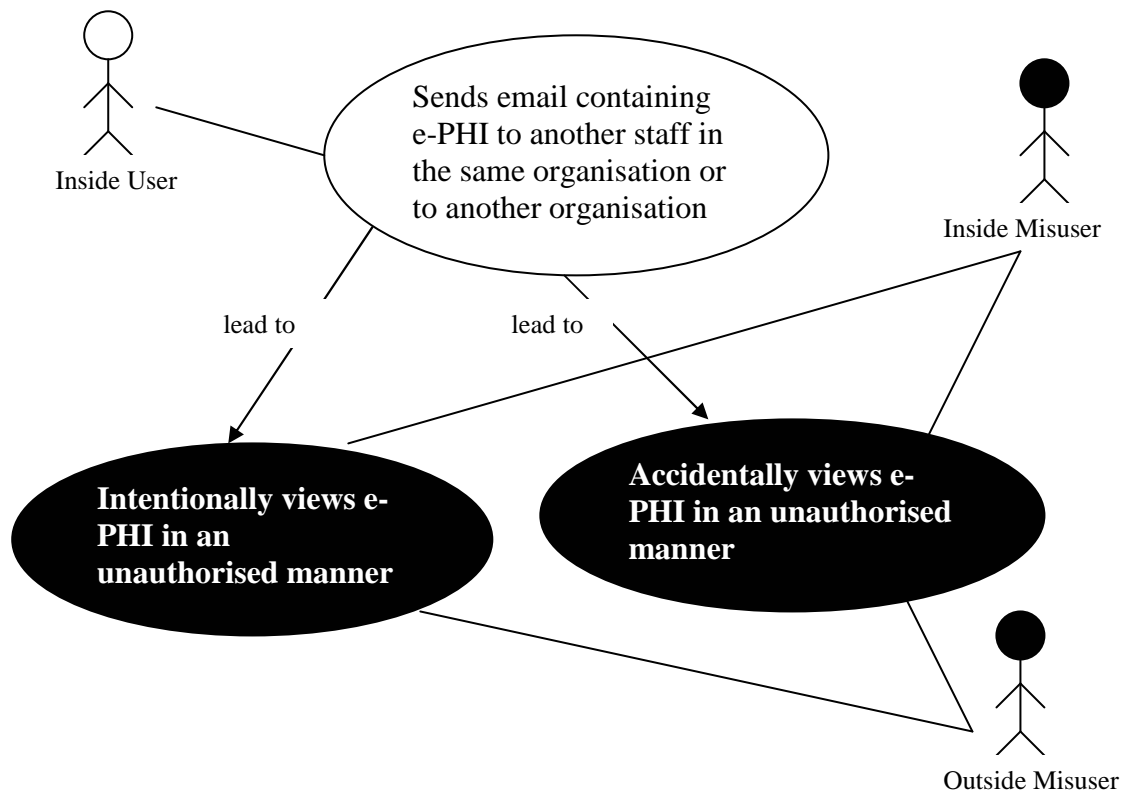


Figure 6.7: Emails containing e-PHI can be misused by both insiders and outsiders.

then it would be a Threat 3 type misuse.

## 6.8 Unauthorised Access Through Unattended Workstation

Two of the respondents, R4 and R6 identified unauthorised access through unattended workstation as a security concern. If a workstation is unattended for a prolonged period of time then it is possible that a misuser steals a large volume of e-PHI or even modifies e-PHI inappropriately. Thus unattended workstations provide an easy way for misusers to violate confidentiality, integrity and availability of e-PHI. Figure 6.8 shows three possible types of misuse cases where unauthorised access is gained through unattended workstations.

This misuse case is an organisational threat since the breach of security occurs within the organisational boundary. Similar to the password sharing misuse case, the range of misuse cases that can result from an unattended workstation is quite big. Once compro-

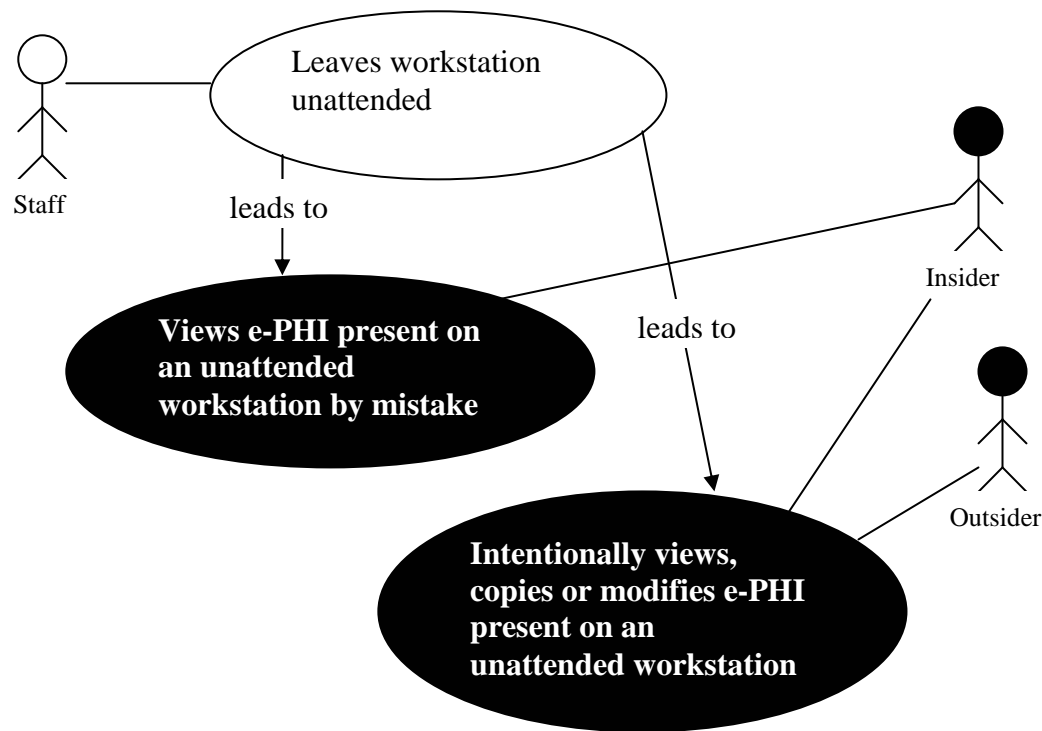


Figure 6.8: Unauthorised access through an unattended workstation.

misused the misuser gains complete access rights of the owner of the workstation.

There can be three types of misuses resulting from unattended workstations. Firstly there are accidental misuses where an innocent insider happens to read someone's e-PHI present on unattended screen by mistake. This will be a Threat 1 (accidental misuse by insiders) type misuse. In this case however the actual consequences of misuse would be minimal. The second type of misuse is carried out by malicious insiders who prey on unattended workstations with the intent of stealing or modifying e-PHI. This will be a Threat 3 (insiders going outside their access rights) type misuse. The adverse consequences can be much more severe with the second type of misuse. Thirdly physical intruders can also gain access to e-PHI through unattended workstations in which case it will be a Threat 4 (unauthorised physical intrusion) type misuse.

## 6.9 Data Inconsistency caused by multiple systems that are not integrated

Two of the respondents, R1 and R6 identified having multiple shadow systems or databases that are not integrated as a security concern. Often to provide redundancy for greater availability shadow systems are used. When multiple systems that contain the supposedly same data are used together, data integrity can be at risk. Tight data integration is critical in such cases to ensure data consistency. Sometimes there can be errors in those integration measures that lead to inconsistent data. Even with the appropriate integration measures, software or hardware failures can cause data inconsistencies across the multiple systems.

This is a misuse case with where the misuser is a non-human entity. Literature on misuse cases allow modeling of non-human entities such as natural disasters as misusers [41]. Figure 6.9 shows a misuse case where unexpected software failure causes inconsistency in e-PHI held in two separate systems.

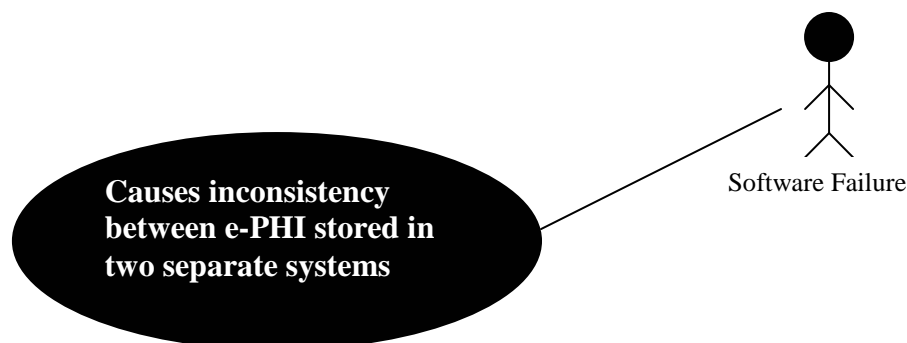


Figure 6.9: Software failure causes inconsistency between e-PHI stored in two separate systems.

Trying to classify this misuse case into the existing taxonomy causes problems. Firstly it is not a systemic threat since no flow of data is involved. Data inconsistency threatens the integrity objective of an organisational policy and thus it can be classified as an organisational threat. However it is not possible to categorise this misuse case as any one of the five threat types because the existing taxonomy does not incorporate the threats where the attacker is not a human being. A software failure is neither an insider nor

an outsider. Moreover it is not appropriate to consider it innocent or intending to harm because it has no motive as such. It occurs due to the design flaws or logic errors that manage the integration of the multiple systems.

## **6.10 Clearinghouse breach that would draw us into investigation**

One of the respondents, R6, identified a security breach at a clearinghouse as a security concern. The actual response shown in Table 6.10 suggests that the concern is about potential investigation that would involve the respondent. Clearinghouses engage in exchange of various e-PHI with dental schools. If a security breach occurs in a clearinghouse it is possible that the related dental schools are drawn into investigation. This misuse case is not an organisational threat because a security breach at a clearinghouse does not directly violate the security policy of a dental school. Because the security breach occurs after successful transfer of e-PHI to a clearinghouse it is outside the control of the school that sent it. The respondent was worried about all the loss of time and resources that a major investigation would incur. This misuse case is a systemic threat since it occurs as a result of the flows of e-PHI between dental schools and clearinghouses.

## **6.11 Suggested improvements to the existing taxonomy**

We tried to categorise the identified misuse cases according to the taxonomy of threats against e-PHI presented in [8]. From our analysis we discovered some gaps in the existing taxonomy.

Password sharing is an organisational threat that can lead to a wide range of potential misuses. While it is clearly a security threat we were not able to adequately categorise it into any of the five types of organisational threats as shown in Section 6.4. When an

attacker compromises a user password using technical or other means to gain access to e-PHI, it falls in either Threat 3 or Threat 5 category. Also when someone accesses e-PHI using a borrowed password, he/she is considered to be committing a misuse. However the current taxonomy does not include the situation where an authorised user shares his/her password with others as a threat on its own. Therefore we suggest that ‘voluntary disclosure of user credentials that leads to unauthorised access’ to be included as another type of organisational threats to e-PHI.

Our examination of the cover-up attempts by insiders also presented a problem. We successfully classified it as a Threat 2 type misuse but we found that the current taxonomy of threat motives cannot adequately categorise potential motives of a cover-up attempt as shown in Section 6.6. Profit, curiosity and spite are the three existing categories of motives for the organisational misusers. We suggest that ‘coverup for mistakes’ be included in addition to the existing three in the taxonomy of potential motives for misusers. This motive is especially important in a medical context as malpractice lawsuits are constantly increasing.

Finally we suggest that non-adversarial threats that results from non-human entities be added to the existing threat taxonomy. Our suggestion is based on our analysis of the data inconsistencies caused by multiple shadow systems in Section 6.9. The current taxonomy cannot categorise the non-human, non-adversarial threats against e-PHI such as errors in software or hardware causing corruption of data because It assumes a human misuser in all five levels of organisational threats.

The new taxonomy of organisational threats with our suggested improvements will be as follows. Our improvements are shown in bold.

1. Threat 1 : Innocent insiders who cause accidental breach of security by mistake.
2. Threat 2 : Insiders who abuse their access rights. The attacker acts within the boundary of his/her access rights to commit the misuse.
3. Threat 3 : Insiders who go outside of their access rights and knowingly access information for spite or for profit. This type of threat arises when an attacker does



not have access to the desired data and through technical or other means gains unauthorized access to that data.

4. Threat 4 : The unauthorized physical intruder causing breach of security.
5. Threat 5 : Rogue employees and outsiders, who mount attacks to the information system. This is a purely technical threat where the attacker has no authorization and no physical access.
6. **Threat 6 : Non-human entities that cause damage to e-PHI.**
7. **Threat 7 : Insiders who voluntarily disclose their user credentials to peers.**

The new taxonomy of motive for misusers with our improvements will be as follows. Our improvements are shown in bold.

1. Economic Reasons
2. Spite
3. Curiosity
4. **Coverup for Mistakes**

## 6.12 Misuse Cases Breakdown

Table 6.11 shows the summary of our cluster analysis in the context of our improved threat taxonomy.

We found that six out of the seven misuse cases are organisational threats. One of the misuse cases, namely disclosure of email containing e-PHI was classified as both organisational and systemic depending on the misuser. In all of the organisational threats insiders were potential misusers. On the other hand only two of the organisational threats involved outsiders. It is interesting to find that none of the threats identified from our

Table 6.11: Taxonomic breakdown of the identified misuse cases

Misuse Case	Type	Threat Type
Password Sharing by insiders	Organisational	7
Inconsistency in e-PHI caused by multiple shadow systems not integrated	Organisational	6
Cover-up attempt by insiders	Organisational	2
Disclosure of email containing e-PHI	Organisational & Systemic	1,3
Unauthorised access through unattended workstations	Organisational	1,3,4
Theft of desktop computers	Organisational	3,4
Clearinghouse breach leading to investigation	Systemic	N/A

survey was a Threat 5 type where a purely technical attack is mounted from an unauthorised misuser. When outsiders were involved they were physical intruders rather than technical intruders. Thus control of insiders proved to be a critical issue for the survey respondents. Only two respondents expressed concern about systemic threats.

## 6.13 Discussion

### 6.13.1 General Findings

In this chapter we analysed the perceptions of the survey respondents regarding the HIPAA technical safeguards as a whole. We highlighted the areas of HIPAA technical safeguards that the respondents were worried about. We made an observation that the levels of concern held by our respondents for the HIPAA standards are not uniform. We made the observation from our survey data that Audit Control standard had the highest mean level of concern followed by Transmission Security. We tested two different hypotheses to establish some statistical significance of our observation.

The first hypothesis was based on the difference between the mean values of the concern levels given by the respondents for each standard. We used Student's t-test for paired data to see if there is enough statistical significance in the differences between the mean values. We could not reject our null hypothesis in our first test. Being aware of the

low statistical power of our test, we suspected a type-II error of falsely retaining the null hypothesis and performed another test.

The second test was based on the rankings of the standards from each respondent. We used a point system to concentrate on the most important standard. Another advantage of using rankings instead of raw concern levels given by the respondents was that it gave equal weighting to every respondent and compensated for the different scales of the respondents. Based on our point system we performed Student's t-test for paired data again to see if the differences are significant. From the test results we were able to conclude at the 95% confidence level, that Audit Control is more important to our respondents than Access Control and Entity Authentication. Also we were able to conclude at the 90% confidence level, that Transmission Security is more important to our respondents than Access Control and Entity Authentication.

However because of the low response rate and resulting bias in our sample, the finding is not conclusive. Nevertheless it is interesting to see that this result agrees with findings of other studies [10, 48] undertaken for other areas of medical industry. They also found Audit Control as the most difficult standard to implement. Thus we believe that our finding can be used as a hypothesis for a future study of the dental schools with a larger, unbiased sample.

We asked the respondents what they think about the potential trade-off between security and patient care. Six out the seven respondents reported that they are not concerned about such trade-off. The one respondent who reported concern about the potential trade-off made indicated that logging features of the information system caused slower response time thereby getting in the way of care. No statistical validity can be asserted for this observation. Nonetheless since Audit Control was identified as causing more concern than other standards, it would be interesting future work to investigate the impact that logging in information systems have on patient care.

### 6.13.2 Misuse Cases

We identified seven different misuse cases from our survey responses. Our misuse case analysis shows that the misuse cases themselves are generic misuse cases that may exist in other, non-health IT related systems that do not manage e-PHI. Password sharing for example is a threat to any information system. What is unique about e-PHI related threats are the potential implications. The implications of an instance of password sharing will differ drastically depending on whose password is shared and which part of e-PHI is affected as result.

We asked for detailed narratives of threat scenarios but the survey responses did not provide enough details for us to conduct in-depth threat analysis without making assumptions about what the respondents might have meant. Often short phrases like ‘password sharing by insiders’ were used. To study the threats in more depth we used misuse case analysis to model the abstract, high-level concerns given the survey responses into more detailed misuse cases after making some reasonable assumptions.

In our cluster analysis we found some gaps in the existing threat taxonomy proposed by the US National Research Council in [8]. We suggested improvements to the existing taxonomy to make it more flexible.

A notable characteristic of the reported misuse cases was that they did not require a high level of technical sophistication. None of the misuse cases described by the respondents were in the Threat 5 (unauthorised technical misuse) category. Attacks such as denial-of-service attack were not considered to be a significant part of the threats by the survey respondents. All of the identified threats required little technical expertise. Until dental information systems are improved to the point that security breaches require significant technical expertise, the only available mitigation for such threats will be stronger deterrence mechanisms for the trusted insiders.



# 7

## Mitigation for Coverup Attempts by Insiders

We presented the survey results and our analysis in Chapter 6. In this chapter we examine how our misuse case, ‘coverup attempts by insiders’ can be mitigated. In Section 7.1 we discuss the possible countermeasures for this misuse case. Then in Section 7.2 we provide the necessary background on audit controls. In Section 7.3 we devise a hypothetical scenario of our misuse case. In Section 7.4 we present an existing guideline, namely RFC 3881 for audit controls in health care information systems. In Section 7.5 we discuss suitability of RFC 3881 for detection of our misuse case. Finally in Section 7.6 we propose use of a workflow-based audit system to detect potential signs of the misuse case.

## 7.1 Need for Audit Controls to Mitigate Coverup Attempts by Insiders

The misuse case where a dentist tries to cover up his/her mistakes was explained in detail in Section 6.6. We classified it as a Threat 2 type misuse case where an authorised insider abuses his/her access rights. Our review of the countermeasures for each level of organisational threats in Section 4.2 identified audit controls as the only technical means by which Threat 2 type misuses can be countered.

Because a dentist has the necessary privileges to modify the records, no amount of authentication or access control will protect against this misuse case as long as he/she acts within the boundaries of his/her access rights. Thus it can be seen that the only possible way is to keep an audit trail of system usage and try to detect such misuse based on the audit trail. It is the task of the enterprise dental information systems to implement appropriate audit controls.

## 7.2 Audit Controls

The term audit is defined as ‘To record and analyze system activity for security problems and vulnerabilities’ in [49]. Audit controls refer to the various mechanisms that enable an audit to be carried out.

Audit is essentially a detection mechanism based on the past record of system activities called ‘audit trails’. It is the last line of defense in Lampson’s gold standard which consists of authentication, authorisation and audit [50]. There are two components in an audit [51].

1. The collection and organisation of audit trail data.
2. The analysis of the audit trails to discover or diagnose security violations.

The first component of audit process is often referred to as ‘logging’ in the literature. Logging of audit trails can occur at various levels such as application, operating system

or network. In theory, it is possible to capture every mouse clicks of every user or every field access in a database. However collection of such complete audit trail will result in performance overheads that will make the system unresponsive or even unusable. This means that any audit trails have to be selective. Therefore the question of what to record is important.

The second component can serve two purposes. Chen et al. make the distinction between forensic and surveillance uses of audit trails in [52]. Forensic use of audit analysis is about determining what went wrong and who was at fault after the detection of a security breach. On the other hand, surveillance use of audit analysis concerns detection of interesting events that might be happening that warrant further investigation. Audit analysis for surveillance purposes can occur after-the-fact or in real-time. In the latter case, the process is usually referred to as ‘intrusion detection’. There are two broad categories of intrusion detection namely misuse-based intrusion detection and anomaly-based intrusion detection [53]. Misuse-based intrusion detection works by looking for specific attack patterns or signatures in the audit trail data. Anomaly-based intrusion detection builds a profile of normal behaviour and looks for any significant deviation from it to detect intrusions. In our analysis we focus on the requirements for surveillance audit controls that will actively detect potential signs of the misuse case.

### 7.3 Hypothetical Scenario of a Coverup Misuse Case

We present a hypothetical scenario of a coverup misuse case to be used in the subsequent analysis.

“A dentist creates an oral diagnosis report and a treatment plan on the dental information system for a patient on date X and Y respectively. On some future date, treatment is provided. Some time after the treatment, the patient suffers from severe side-effects. The dentist who became aware of this problem fears the possibility of a malpractice lawsuit and decides to modify the diagnosis report and treatment plan inappropriately to his advantage. This after-the-fact modification takes place on date Z which is a month after



date Y.”

In the following sections we examine how existing guidelines for audit control implementation can detect the misuse case described above.

## 7.4 Existing Requirements for Audit Controls

In this section we review the existing requirements for audit controls and discuss whether they are capable of detecting the coverup misuse case.

### 7.4.1 HIPAA Provisions On Audit Controls

HIPAA’s audit control standard does not specify any implementation specifications. Please refer back to Section 2.2 for the definition of the standard as specified by HIPAA. Under HIPAA it is up to the individual covered entities to decide how to implement their audit controls. Since the provisions specify so little in terms of actual implementation, it is impossible to discuss whether the provisions can effectively detect the misuse case in discussion.

### 7.4.2 RFC 3881

Although it is impossible to define an auditing system in enough detail to suit every organisation, there are a number of different guidelines as to what is required of a health care auditing infrastructure [54, 55, 56, 57].

RFC 3881 attempts to consolidate the disjoint viewpoints from these different guidelines [58]. It proposes a set of trigger events and corresponding data definitions for the events to be captured by a health care information system. They are briefly outlined in the following subsections. By presenting a common data schema for audit trails for e-PHI it tries to achieve interoperability among heterogeneous application systems.

### **Security Administration Events**

This class of trigger events includes all actions that create, maintain, query, and display definitions for securing data, functions, and the associated access policies. Examples of security administration events include user/role/permission definition.

### **Audit Administration and Data Access Events**

This class of trigger events includes all actions that involve the collection and management of audit trails. Examples include audit data access and audit data modification/deletion.

### **User Access Events**

This class of trigger events includes events of access to secured data and functions for which audit data might be collected. These events are further categorised into e-PHI events and non-e-PHI events.

1. E-PHI Access Events : E-PHI-related events are events that directly involve e-PHI. They include create, modify, view and delete events.
2. Non-e-PHI Events : Non-E-PHI events are events that occur during routine operation of an IT system that are not directly related to e-PHI. However even routine events can become abnormal if they happen under specific circumstances, perhaps depending on the local situation. Examples of this type of user access events include machine startup/shutdown, failed login attempts and automatic logout.

### **Data Definitions For Audit Trigger Events**

Audit trails containing only the events are unlikely to achieve the overall goal of investigative usefulness. [58] suggests including following event details.

1. Date and time of the event
2. ID of the user who caused the event

3. The application that created the audit event
4. Workstation where the event happened
5. Description of the event

## 7.5 Detection of the Coverup Misuse Case using RFC 3881

RFC 3881 defines a comprehensive data model for health information audit trails. However it does not concern itself with the analysis of the audit trails. We examine if the audit trails recommended by RFC 3881 capture sufficient information to enable detection of our misuse case.

Security Administration events are important but they do not capture our misuse case or directly aid in its detection because they do not concern the e-PHI access of the legitimate users. Similarly audit related events and user access events that do not involve e-PHI are not relevant for countering our misuse case.

The user access events that involve e-PHI are relevant because they capture the events of the misuse case. Following are the hypothetical audit events generated by a RFC 3881 compliant audit system for our misuse case. We will end up with three separate data access records.

Table 7.1: Three Data Access Records Resulting From Our Hypothetical Misuse Case based on RFC 3881 recommendations

Event Details	Event1	Event2	Event3
Date/Time	X	Y	Z
User ID	John	John	John
Application	IS	IS	IS
Workstation	1.1.1.1	1.1.1.1	1.1.1.1
Description	oral diagnosis for patient A	treatment plan for patient A	Modification of e-PHI for patient A

The audit trails will record which user has accessed which data on what date. If an investigation for a malpractice is already in progress, the examination of the above audit

trails will reveal that on Date Z, there was some modification of the e-PHI. However for the surveillance purposes the above audit trails do not capture enough details. Without manual investigation of the audit trails there is nothing to differentiate the access on Date Z from the accesses on Date X and Y. In the given audit trails the only thing to indicate that the access on Date Z is suspicious is the fact that there is some time difference between Date Y access. However in the audit trails there is no information specifying the relationship between the three events. For example the time difference between Date X and Date Y events is legitimate because there is some relationship between the nature of the events that specifies one happens after the other. Timing information of the events by itself is not enough detect signs of the misuse case. Therefore we conclude that the audit trails defined in RFC 3881 are not sufficient to support proactive detection of our misuse case.

## **7.6 Workflow-based Audit Controls for Countering the Coverup Misuse Case**

In the previous sections we looked at the existing audit control guidelines and found that they do not capture enough information to realise detection capabilities of a surveillance purpose audit system. Even ignoring the performance overheads and considering the case where every e-PHI related access is recorded revealed limitations in detecting our misuse case.

We pointed out in Section 7.5, the need for capturing the relationships between the data access events for successful detection of our misuse case. We examine the potential use of clinical workflow-based audit controls as a solution to this problem. Workflow is a term often used in the literature to refer to a subset of business processes whose execution is supported by information technology. Workflow Management Coalition defines workflow as “The automation of a business process, in whole or part, during which documents, information or tasks are passed from one participant to another for action, according to

a set of procedural rules” [59].

A workflow model consists of the five basic building blocks as shown in the list below [60].

1. Workflow Processes
2. Activities
3. Transitions between activities
4. Participants
5. Relevant Data

Workflow processes correspond business flows. They consist of one or more separate activities. Transitions between activities refer to the progression or execution of a workflow process. Each activity is performed by designated participants using relevant data as input. Workflow modeling consists of creating a workflow schema using the above building blocks and then having instances of the schema with a particular state at any given point in time.

A clinical workflow refers to the flow of events in which care is delivered to patients [61]. Figure 7.1 shows a hypothetical workflow for a dental treatment and demonstrates how our coverup misuse case can be detected.

There are four activities within our workflow process for a dental treatment. The e-PHI of the patient involved is the data for the activities. Firstly a receptionist makes the booking for the patient. Then the dentist sees the patient and creates an oral diagnosis. Once the diagnosis is complete the dentist can put together a treatment plan and then provide treatment accordingly. The final activity of the workflow process is the checkup that occurs some time after the actual treatment. The sequential order in which the transitions to and from activities happen is defined and any deviation from that order is considered as an anomaly or an exception in the workflow execution. Our misuse case is shown as an anomaly in the Figure 7.1 as activity transition arrows going up instead of down. An anomaly as such can be used to raise an alarm to warrant further investigation.

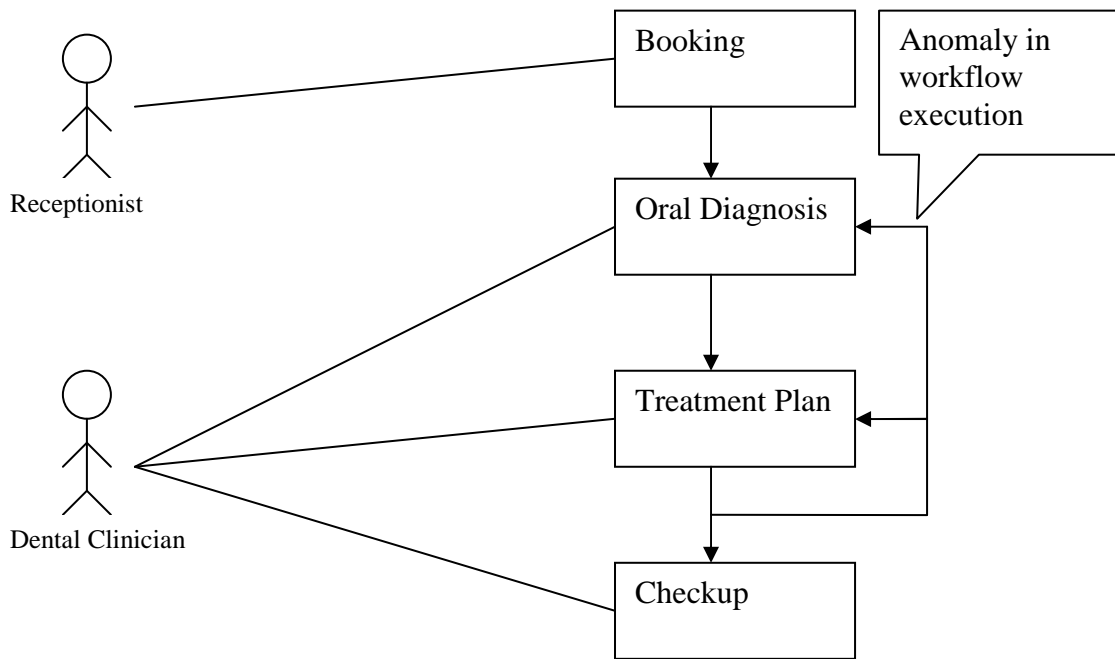


Figure 7.1: A hypothetical workflow for dental treatment. After-the-fact modification is treated as an anomaly in the workflow execution.

Another possibility is to use the workflow model as an access control mechanism. By strictly enforcing the sequential order of the activities it would be possible to prevent the misuse case. For example, if this method is used the context of our misuse case, the dentist would not be allowed to modify the e-PHI once he/she completes the initial diagnosis and treatment plan. However suitability of this rigid approach is questionable in a dental context. It is generally considered to be a bad practice to use restrictive measures for controlling the behaviour of the health care providers because they have adverse impact on their ability to deliver quality care. Dadam et al. argue that variations in the course of a pre-planned treatment process are deeply inherent to medicine to the extent that it is normal for unforeseen events to occur[62]. For example in our case, it is possible that the patient requires some urgent treatment resulting from an emergency. In an emergency situation like this, there may be no time to write up an oral diagnosis report. Having a rigid workflow-based information system that is restrictive will not handle this situation well. It is also believed that such systems will not gain acceptance from the health care professionals.

In an audit system for surveillance purposes instead of restricting user behaviour, users

are allowed to perform whatever activity within their access rights but if their behaviour deviate from the defined workflows such deviations are recorded. An enterprise dental information system that implements an audit system as described will need to record the e-PHI access events together with the information about the workflow instance to which it belong. When the anomaly discussed in Figure 7.1 occurs, it can be recorded as an activity that did not belong to any particular workflow instance.

The audit trails that contain workflow related information about the e-PHI access events can then be analysed to detect the misuse. An important consideration for the detection is the false positive rate. Given the nature of dental care provision, some anomalies in the workflow execution will be caused by genuine variations in the process of dental care. Therefore it is important to devise ways to reduce the false positive rate.

Discussion of workflow-based audits in the literature mostly concern the process monitoring for optimisation purposes. They advocate collection of various statistics on the workflow executions to improve the efficiency of an organisation's operations. Handling of exceptions in workflow executions is an active research area. However current works on workflow exceptions mostly concern how they can be handled efficiently with minimal loss for the organisation. To date we have not found any work that uses workflow exceptions to detect insider misuses.

## 7.7 Discussion

In this chapter we examined possible countermeasures for one of the misuse cases identified from our survey where an authorised insider attempts to coverup for mistake. We argued that implementation of effective audit controls is the only technical means to counter the misuse case. The word 'technical' is an important qualification for our argument since there is a variety of administrative means to deter insider misbehaviour such as education and sanction policy.

Following our argument, we reviewed RFC 3881 which is a set of guidelines for security auditing in health care information systems. The focus of our analysis was to see if the

RFC 3881 guidelines are sufficient to proactively detect our misuse case. Our analysis showed that the audit trails recommended by RFC 3881 do not capture enough data to detect potential signs of our misuse case.

We proposed a workflow-based audit system to mitigate our misuse case. We showed that it would be possible to detect our misuse case by looking for anomalies in workflow executions. Implementing this type of audit controls imposes an important requirement on the way that information systems are designed. Information systems and their underlying data models should be designed in such a way that they are aware of the workflow schema and individual instances. Furthermore they should have capabilities to automate their executions so that any manual overrides by staff can be recorded. Graber refers to systems with these characteristics as ‘workflow management systems’ in [61].

There are some open issues to be addressed before our brief proposal can become a practical feasibility. Firstly performance issues have to be addressed. To simplify our analysis we did not concern ourselves with the performance issues related to managing and recording workflow-based information. Workflow related information is additional information that has to be recorded so we expect an impact on the system performance. Thorough investigation of performance issues should be carried out.

Secondly false positive rate of our proposed system is also an important concern. As we have mentioned earlier, exceptional situations are common in medical environment. We expect that our simple detection method of treating any anomalies in workflow execution as sign of misuse would lead to a high false positive rate. We believe that false positive rate is closely related to acceptance by the medical professionals so it is important to find ways to better differentiate the misuses from genuine deviations.





# 8

## Conclusions and Future Work

In this chapter we outline the conclusions that resulted from this study and suggest avenues for future work.

### 8.1 Conclusions

In this thesis we investigated the security requirements for enterprise dental information systems held by the US dental schools.

In Chapter 2 we outlined the provisions of the HIPAA Security Rule that lacked sufficient specificity regarding implementation of the various technical controls. The existing HIPAA provisions are aimed to adequately protect e-PHI. The requirements imposed by the provisions do not prescribe particular implementation or detailed threat model which

to be countered. We characterised various aspects of a typical enterprise dental information system for which we set out to elicit security requirements. Main user groups and their business flows were identified. We showed that our system utilises e-PHI in the process of supporting the various business processes of its users. We outlined the need for more detailed security requirements for these systems.

In Chapter 3 we examined the existing methodologies for engineering requirements. Our focus was on the methodologies that were driven by the end user requirements. This was due to our goal which was to elicit the requirements held by the the end-users of the dental information systems, namely the US dental schools. From our review we identified goal-based, scenario-based and viewpoint-based approaches as the three general categories of requirement engineering methodologies that use end user perceptions for elicitation of requirements. Our evaluation showed that scenario-based RE methodology is the most suitable option for our research.

We outlined some of the differences between functional requirements and security requirements which reduce effectiveness of more common methods such as use cases for capturing security requirements. We identified threat modeling as a general approach to capture security requirements in the form of negative scenarios or threats. We reviewed and evaluated two distinct techniques for threat modeling namely misuse case analysis and attack trees.

We compared the elicitation techniques for functional requirements and security requirements suggested in the literature. We found that unlike in the scenario-based RE methodologies for functional requirements, there is a lack of user-driven elicitation techniques for security requirements. All the techniques that we reviewed relied on the security analyst to work out the potential threats rather than trying to understand the end-user perceptions.

In Chapter 4 we reviewed an existing taxonomy of threats against e-PHI. From our analysis, we verified the claim made by another work that systemic threats cannot be countered by technical countermeasures alone. We agreed with the argument that industry-wide standardisation efforts are necessary to effectively mitigate systemic threats. We

compared the proposed countermeasures for each type of threat found in [8] with the standards of the HIPAA technical safeguards. We found that while there are overlaps between the two sets of security controls, HIPAA standards offer a more extensive and fine-grained set of technical countermeasures.

In Chapter 5 we described and justified our survey methodology with respect to our objectives and constraints. Our objective of eliciting user requirements for security drove our data collection requirements. Further our time and geographic constraints meant that an online user survey would be the most suitable. As we found from our review of the literature, approaches to understand the user perceptions about the security threats are relatively rare. Thus our experimental hypothesis was to see how effective a survey-based methodology can be for elicitation of security threats. We also outlined the response rate for our survey and the data analysis methods which were used to reach our findings.

In Chapter 6 we presented our survey data and analysis that led to our findings. Firstly we found that the area of HIPAA that our survey respondents were most concerned about is Audit Controls, followed by Transmission Security. Due to the low response rate of our survey this result is not conclusive. One of our statistical tests indicates that this result is not likely to be caused by pure chance. Other works have reported similar finding, increasing our confidence in the validity of this result.

In our analysis, we identified seven security threats or misuse cases which the survey respondents considered as being important for their HIPAA compliance. The misuse cases were based on the unstructured responses that described scenarios of non-HIPAA-compliant system use. The misuse cases themselves were generic threats applicable in other domains of information security. However the implications and the motives of these misuse cases in the dental context were unique.

We performed cluster analysis to see if the existing taxonomy of threats is capable of containing our misuse cases. During our analysis we found some gaps in the existing taxonomy. To plug these gaps, we proposed two new threat types and one modification. Our new threat types are listed below.

1. Voluntary disclosure of user credentials by authorised insiders
2. Non-adversarial threats caused by non-human entities

We argued that coverup attempts for mistakes were not necessarily motivated by economic reasons. Other factors such as a desire to avoid embarrassment or a loss of reputation may be important. Therefore we proposed that coverup for mistakes be included as a third type of misuser motive, in addition to spite and curiosity.

In none of our seven misuse cases was technical means employed by an unauthorised outsider. Most of the misuse cases identified by our survey respondents required little technical sophistication and were committed by trusted insiders. This result cannot be generalised to all US dental schools because of the low response rate. However we believe that it would be an interesting hypothesis that can be verified in future work.

In Chapter 7 we proposed a mitigation for one of the misuse cases identified from our survey. In this misuse case, a dentist modifies e-PHI after-the-fact to hide an omission. Our analysis demonstrated that the only possible countermeasure for this type of insider misuse is to implement sufficient audit controls to enable effective detection. We distinguished the use of audit controls for surveillance purposes from their use for forensic purposes. We concentrated on audit controls for surveillance purposes which require proactive detection of potential misuses. We found that RFC 3881 which is a guideline for health care information does not adequately meet this requirement for proactive detection. This inability arises because the relationships between the individual e-PHI access events are not captured in the suggested audit trails. To improve this situation we proposed a workflow-based approach to audit user access events. In the proposed approach the individual access events are logged with the context information about the workflow instances to which they belong. Then we showed that it would be possible to detect the misuse case by looking for any anomalies in the workflow execution. We outlined some of the implications of implementing such audit controls on the information system design. We also discussed potential issues regarding the false positive rates of our approach.

One of our experimental hypotheses was that our survey-based misuse case analysis

would result in more detailed security requirements than the existing legal provisions. Because of the low response rate of the survey, it is difficult to generalise about these results and confirm the hypothesis yet. Our survey-based methodology was successful in eliciting some specific threats, i.e. some misuse cases that the dental schools perceived to be important for complying with the technical safeguards of HIPAA.

The main motivation for this study was the lack of information regarding security requirements under HIPAA, as perceived by US dental schools held by a local information system exporter. Our results are expected to be of interest to dental information system vendors who are confused about the security requirements held by the dental schools. By considering some of our misuse cases, technical controls that can effectively mitigate them can be developed. Also our findings are expected to be of interest to the dental schools themselves. Informing them of some of their peers' security concerns can aid each dental schools in their compliance process.

The practical implications of the security threats identified in this thesis are limited because they cannot be generalised to the target population. Because of our small sample size, we cannot be confident that any of our findings are broadly representative of our target group. Despite this limitation we believe that the findings of this exploratory study are valuable hypotheses which could be verified in future studies of similar kind.

## 8.2 Future Work

This thesis has identified some avenues for future work. Any of the findings from our exploratory study might be verified in a more focused study with larger sample size. The response rate for our survey was 12.5%, despite all our efforts to attract more responses. We speculated that the length of the survey, the number of open-ended questions and the reluctance to disclose sensitive security related information were some of the factors that caused the low response rate. The relatively long survey was a result of our desire to explore a wide range of user perceptions. A high proportion of our questions were open-ended because we did not want to bias the user responses by providing specific

choices. However in future work, we would advise a more focused approach where some of the hypotheses formulated from our work are tested using more questions that require structured responses. We believe that such approaches will improve the response rate. Using more direct data collection techniques such as interviews or phone interviews might reveal interesting results.

Our work was limited to dental schools but it would be worthwhile to extend the target population of the study to the wider health care industry. This would allow future researchers to compare the security requirements held by different types of HIPAA covered entities.

Another approach would be to focus on one institution and study the perceptions of the different user groups within an organisation. Our work assumed that our respondents' perceptions are representative of the dental school that they belong to. It may be true that there are differences between the different user groups. More focused investigation into specific areas of HIPAA such as Audit Controls would also be worthwhile.

Our investigations were focussed on user perceptions, but it would be interesting to investigate the technical feasibility of our proposed workflow-based audit controls. A prototype implementation of a workflow-based anomaly detection system is a possibility. Another possible research direction is to find ways to differentiate misuses from legitimate anomalies in the workflow execution.



## **Survey Instrument**

### **Survey - HIPAA's Security Requirements**

There are varying interpretations of the HIPAA's security rules by different providers. This survey is intended to gather useful information about such interpretations thereby allowing better security requirements to be elicited for the health IT systems. If your organisation has conducted some form of risk analysis previously, please provide us with the results as this would be extremely helpful to our research. We intend to publish the aggregate survey results. Please note that the results published will preserve anonymity.

### **Respondent Details**

Institution : Role :



## Technical Safeguards

### *General*

1. Please number each area of the HIPAA security rule listed below in order of your level of concern in terms of existing system compliance. (5 for Very concerned and requires immediate attention to 1 for Not concerned at all)

Access Control (access policy, user id etc)

Transmission Security (electronic transmission of patient data eg.email)

Audit Control (recording user activities for detection of security breach)

Data Integrity (making sure data is not altered or destroyed in unauthorized way)

Entity Authentication (verifying that an entity seeking access to patient health information is actually the one claimed to be doing so)

2. Do you think your organization has security issues in the way of patient care? If yes, please explain briefly.
3. Have you identified any security vulnerability of your current information system with regard to HIPAA? If yes, please describe one that you are most concerned about.
4. Does your information system currently interact with any external systems? (eg.Clearinghouse, insurance companies) If yes, please describe a scenario of the biggest perceived threat that arises while your system is interacting with the outside world.
5. Do you consider insider attacks as being a significant part of the threats? Please describe a scenario of a likely insider attack that you are concerned about.

### *Access Controls*

Unique User Identification

6. Are you satisfied with the way that your current information system handles user identification with regard to HIPAA security rules? If not, please explain briefly.

- 
7. Please describe a scenario of system use related to your current unique identification approach that you view as being non-HIPAA-compliant (Please specify in a list of steps of 'who will do what').

Here is a very simple, sample scenario

"A student logs in using his friend's unique ID and password " He/She modifies some fields in a patient's dental record " He/She logs off.

*Emergency Access*

8. Are you satisfied with the way that your current information system handles emergency access with regard to HIPAA security rules? If not, please explain briefly.
9. Please describe a scenario of system use related to your current emergency access feature that you view as being non-HIPAA-compliant.

*Automatic Logoff*

10. Are you satisfied with the way that your current information system handles automatic logoff with regard to HIPAA security rules? If not, please explain briefly.
11. Please describe a scenario of system use related to your current automatic logoff feature that you view as being non-HIPAA-compliant.

*Transmission Security*

12. Are you satisfied with the way that your current information system handles transmission of patient health information with regard to HIPAA security rules? If not, please explain briefly.
13. Please describe a scenario of system use related to your current transmission mechanisms that you view as being non-HIPAA-compliant.
14. Do you think HIPAA requires encryption of patient health information? If yes, please list the situations where you think encryption is appropriate. If not, have you identified any other means to preserve transmission security? Please list them.

15. Do you think encryption of patient health information would compromise availability of the data and get in the way of patient care?

*Audit Control*

16. Are you satisfied with the way that your current information system handles recording of user interactions with regard to HIPAA security rules? If not, please explain briefly.

17. Do you think dental information systems need to maintain an application-level log of user activities that is separate from database and OS level logs ?

18. Have you identified what information needs to be recorded for HIPAA compliance?  
If yes, please list them

19. Please describe a scenario of system use that you view as being non-HIPAA-compliant that your current information system will NOT record.

20. Please describe a scenario of a non-HIPAA-compliant use with regard to the audit control rule that a desirable information system would RECORD.

*Integrity*

21. Are you satisfied with the way that your current information system's electronic mechanisms to corroborate that a patient health information has not been altered or destroyed in an unauthorized manner? (Digital signatures, checksums etc) with regard to HIPAA security rules? If not, please explain briefly.

22. Have you identified any electronic mechanisms to preserve integrity of patient information in a HIPAA-compliant way? If yes, please list them

23. Please describe a scenario of system use related to integrity of patient health information that you view as being non-HIPAA-compliant.

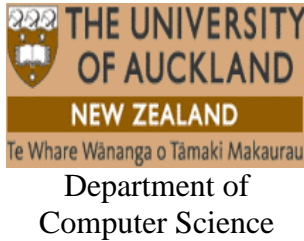
*Entity Authentication*

24. Are you satisfied with the way that your current information system handles entity authentication (verifying that an entity seeking access to patient health information is the one claimed to be doing so) with regard to HIPAA's security rule? If not, please explain briefly.
25. Please list the means in which your organization authenticates users (eg. Biometrics, userID/Password, smart cards, telephone callbacks etc).
26. Please describe a scenario of system use that you view as being non-HIPAA-compliant that will lead to an invalid authentication.



**B**

**Ethics Approval from the University of  
Auckland**



## Participant Information Sheet



UTHSCSA  
Dental School

Title : An Investigation of HIPAA Security Requirements for the US dental schools

Researchers : Professor Clark Thomborson / Jinho Lee / Dr Gary Guest

This research is being undertaken as part of a ME(Master of Engineering) thesis work at the school of engineering by Jinho Lee at the University of Auckland, NZ in collaboration with Dr Gary Guest at the University of Texas Health Science Center at San Antonio Dental School. There are varying interpretations of the HIPAA security rules among different health providers. The provisions have been written in a very general and broad manner deliberately to ensure high applicability. This research aims to investigate such interpretations among the dental schools in the USA. It is hoped that the results of this research will allow better security requirements to be specified for dental IT systems. Also it is expected to broaden the understanding of security issues relating to patient information and then provide some technical recommendations.

Our research involves the distribution of a questionnaire to gather dental schools' understanding of the relevant provisions. Dr Guest, as a member of the ADEA section for Dental Informatics, kindly offered to use his access to the ADEA listserv in identifying potential respondents. Through this listserv your organization has been selected as a potential participant.

Confidentiality will be preserved throughout the research process. If the information you provide is reported or published, this will be done in a way that does not identify you as its source.

Aggregate results will be made available to participants. Also participants will be allowed to request access to preliminary results via Dr Guest. Consent form will have his email address so should you wish to request such access, you can do so.

The information you provide will be stored for a period of six years for the purpose of possible further research. After that period the information will be destroyed by electronically deleting them from the media in which the information was stored.

Please note that as a participant you have the right to withdraw from the project at any time. Also you have the right to withdraw your information/data up to 15 Dec 2005.

Figure B.1: Page one of the Participant Information Sheet

This research is funded by New Economy Research Fund of New Zealand, contract UOAX0214, “Software techniques and systems for the protection of intellectual property”.

It is anticipated that participation in the questionnaire will take no more than one hour.

### Contacts

Professor Alan Williamson (Head of Department)  
+64 (9) 373-7599 ext87922, ag.[williamson@auckland.ac.nz](mailto:williamson@auckland.ac.nz)

Dr Gary Guest (Co-researcher)  
+1 (210) 567-3360, [guest@uthscsa.edu](mailto:guest@uthscsa.edu)

Professor Clark Thomborson (Primary Investigator)  
+64 (9) 373-7599 ext85753, [cthombor@cs.auckland.ac.nz](mailto:cthombor@cs.auckland.ac.nz)

Jinho Lee (Master of Engineering Student)  
+64 (21)781218, [jlee141@ec.auckland.ac.nz](mailto:jlee141@ec.auckland.ac.nz)

If you have any concerns of an ethical nature you can contact the Chair of the University of Auckland Human Participants Ethics Committee at (+64)9,3737599 ext 87830, Private Bag 92019, Auckland, New Zealand.

APPROVED BY THE UNIVERSITY OF AUCKLAND HUMAN PARTICIPANTS  
ETHICS COMMITTEE ON 12 October for 3 Years from 12 October 2005 to 12 October  
2008, Reference Number 2005/362.

[Continue](#)

Figure B.2: Page two of the Participant Information Sheet





Department of  
Computer Science

### Participant Consent Form



UTHSCSA  
Dental School

Title : An Investigation of HIPAA Security Requirements for the US dental schools

Researcher : Professor Clark Thomborson / Jinho Lee / Dr Gary Guest

- I have read the Participant Information Sheet and agree to its terms
- I agree to take part in this research
- I understand that this consent form will be stored for a period of six years in an electronic media(CD-ROM) before it is destroyed
- I understand that any information I provide will be stored for a period of six years before it is destroyed
- I understand that I am free to withdraw from the research at anytime
- I understand that I have the right to withdraw my information/data up to 15 December 2005

Please email Dr Gary Guest ([guest@uthscsa.edu](mailto:guest@uthscsa.edu)) if you wish to request preliminary results of this research.

APPROVED BY THE UNIVERSITY OF AUCKLAND HUMAN PARTICIPANTS ETHICS COMMITTEE ON 12 October for 3 Years from 12 October 2005 to 12 October 2008, Reference Number 2005/362.

[I agree.](#)

Figure B.3: Participant Consent Form

# C

## Raw Data From The Survey

Table C.1: Respondent Roles (Institutions were anonymised)

Respondent	Institution	Role
1	1	Clinic Administration
2	2	HIPAA Officer
3	3	Clinic Administration
4	4	CIO
5	5	Clinic Administration
6	6	Clinic Administration
7	7	Clinic Administration

**Question 1**

Standard	R1	R2	R3	R4	R5	R6	R7
Access Control	2	3	2	1	2	4	1
Transmission Security	2	4	1	5	3	4	1
Audit Controls	4	4	3	5	2	3	2
Integrity	2	3	2	1	2	5	2
Entity Authentication	3	3	nr	1	2	3	2

**Question 2**

Respondent	A02	A02TEXT
1	yes	logging activity
2	no	
3	no	
4	no	
5	no	
6	no	
7	no	

**Question 3**

Respondent	A03	A03TEXT
1	yes	password sharing
2	no	
3	no	
4	yes	Digital Insurance Claims
5	yes	Patient data kept on desk computers, rather than kept on the college server. the theft of a desktop computer caused notifying several hundreds of patients.
6	no	
7	no	

**Question 4**

Respondent	A04	A04TEXT
1	yes	vendor compliance
2	no	
3	no	
4	no	
5	no	
6	yes	Clearinghouse could have security breach that would draw us into investigation or lawsuit.
7		

**Question 5**

Respondent	A05	A05TEXT
1	no	students with prior database admin experience
2		
3	yes	Only if by IT personnel with acces to security clearances
4	yes	Students logging on and then leaving the workstation unattended.
5		
6	No	
7		

**Question 6**

Respondent	A06	A06TEXT
1	no	would like to use 2 tier ID (smart cards)
2	yes	
3	yes	
4	yes	
5	yes	
6	yes	
7	no	I would like to something you have, such as a ID card, and not something you know, such as a password for user identification.

**Question 7**

Respondent	A07TEXT
1	concern for share of password, concern on who is also behind screen when system accessed remotely. Other factors need to be is who can just view VS who can make changes and the nature of the information (ie health history may contain more sensitive information)
2	
3	No such concerns to date.
4	Current system only allows students read only access. Only staff in secure areas have read write privileges
5	as you describe
6	None. It seems unlikely a student would to something malicious using a password provided by a friend.
7	

**Question 8**

Respondent	A08	A08TEXT
1	yes	designated system administrators and service agreement with HIPPPAA compliant vendor has addressed all situations
2		
3	yes	
4		
5	yes	
6	yes	
7	yes	

**Question 9**

Respondent	A09TEXT
1	None to date
2	
3	None to date
4	
5	
6	none
7	

**Question 10**

Respondent	A10	A10TEXT
1	no	JAVA client depends on staying connected, difficulty
2	yes	
3	yes	
4	no	Our existing system does not log off.
5	yes	
6	yes	
7	yes	

**Question 11**

Respondent	A11TEXT
1	see previous answer
2	
3	None to date
4	Students logging on and then leaving the workstation unattended.
5	
6	In some locations, the computer might be on longer than it should before logging off.
7	

**Question 12**

Respondent	A12	A12TEXT
1	yes	point to point encryption with proprietary encryption scheme
2		
3	yes	
4	no	We are soon to replace our system with a new HIPAA compliant system.
5	yes	
6	yes	
7	yes	

**Question 13**

Respondent	A13TEXT
1	we follow prescribed guidelines with transmission of insurance information
2	
3	We do not transmit patient info outside of our own system. We will address the issue when we decide to transmit outside of our system.
4	We do not use our system for transmissions
5	
6	Users sometimes send patient information in emails to outside people. I am not worried about emails being electronically intercepted, which is rare. I am worried that the recipient will not protect the email by leaving a computer exposed, by printing it
7	

**Question 14**

Respondent	A14	A14TEXT
1	yes	remote access or transmission
2		
3	no	We don't yet transmit outside of our own system.
4	yes	Transmission to remote sites (outside our firewall) would require database data encryption or transmission through a vpn.
5		
6	yes	Ideally emails sent outside the school should be encrypted. We haven't figured out how to do this.
7	yes	email

**Question 15**

Respondent	A15
1	yes
2	yes
3	no
4	yes
5	yes
6	no
7	no

**Question 16**

Respondent	A16	A16TEXT
1	yes	no
2		
3		
4	no	Current system does not maintain a historic record of table/field access.
5	yes	
6	yes	
7	yes	

**Question 17**

Respondent	A17
1	our university rules more stringent
2	yes
3	yes
4	yes
5	
6	yes
7	

**Question 18**

Respondent	A18	A18TEXT
1	yes	Ideally would log anytime non-assigned (to that patient)
2	no	
3	yes	
4	yes	Date Time User ID Table Field FieldValue
5		
6	yes	We log each time a user accesses a patient and module (function).
7		

**Question 19**

Respondent	A19TEXT
1	user, patient, file accessed (on individual patient)
2	
3	
4	Our current system is not HIPAA compliant
5	
6	
7	

**Question 20**

Respondent	A20TEXT
1	Our current systems performance is significantly degraded when logging is turned on. Vendor has been notified.
2	
3	
4	Faculty orders a student to modify a treatment plan
5	
6	see #18
7	

**Question 21**

Respondent	A21	A21TEXT
1	no	limitations of java vs a true client-server application
2	no	
3	yes	
4	no	Current system is not HIPAA compliant
5	nr	
6	yes	
7		

**Question 22**

Respondent	A22	A22TEXT
1	no	eliminate shadow systems, have one CIS system establish who the patient is an current demographics them feed other systems.
2	no	
3		
4	yes	
5		
6	yes	
7		



**Question 23**

Respondent	A23TEXT
1	having multiple clinic info systems that are not integrated
2	
3	
4	A user attempting to modify the health record to hide an omission that led to an adverse outcome.
5	
6	Some academic departments maintain shadow databases that might not be secure.
7	

**Question 24**

Respondent	A24	A24TEXT
1	no	would like to implement smart card or biometrics
2	yes	
3	yes	
4	yes	
5	yes	
6	yes	
7	yes	

**Question 25**

Respondent	A25TEXT
1	ID/password ; USB dongle
2	ID/password
3	ID/password
4	ID/password
5	ID/password
6	ID/password
7	ID/password

**Question 26**

Respondent	A26TEXT
1	Faculty password compromised
2	
3	An authorized person sharing their password with someone else. This is non-compliant with our Medical Center confidentiality agreement that is required annually to maintain access to our system. Such non-compliance carries significant internal penalties.
4	Students or Faculty sharing User ID / Password with peers.
5	
6	Cards are easily transferred between people and are unsafe without passwords. They also get lost.
7	

# Bibliography

- [1] United States Department of Health and Human Services, *Health Insurance Reform: Security Standards; Final Rule*, 2003.
- [2] R. Cushman, *Information and Medical Ethics: Protecting Patient Privacy*, IEEE Technology and Society Magazine **15**, 32 (1996).
- [3] T. Huston, *Security Issues for Implementation of E-Medical Records*, Communications of the ACM **44**, 89 (2001).
- [4] K. Kerr, *The Electronic Health Record in New Zealand*, Health Care and Informatics Review Online **8** (2004).
- [5] D. Brailer, N. Augustinos, L. M. Evans, and S. Karp, *Moving Toward Electronic Health Information Exchange: Interim Report on the Santa Barbara County Data Exchanged*, Technical report, California Healthcare Foundation, 2003.
- [6] D. J. Brailer and E. L. Terasawa, *Use and Adoption of Computer-Based Patient Records*, Technical report, California Healthcare Foundation, 2003.
- [7] K. T. Win and J. Cooper, *Information Age, Electronic Health Record and Australia Healthcare*, International Journal of the Computer, the Internet and Management **12**, 14 (2004).

- [8] N. R. Council, editor, *For the Record: Protecting Electronic Health Information*, Washington DC: National Academy Press, 1997.
- [9] G. Allum, private communication, 2005.
- [10] J. Goedert, *HIPAA Security: The Home Stretch*, Health Data Management **13**, 88 (2005).
- [11] S. Northcutt, editor, *HIPAA Security Implementation*, Sans Press, 3rd edition, 2004.
- [12] A. D. Feld, *The Health Insurance Portability and Accountability Act (HIPAA): Its Broad Effect on Practice*, The American Journal of Gastroenterology **100** (2005).
- [13] R. Walker, *A HIPAA Strategy for Dental Schools*, Journal of Dental Education **66**, 624 (2003).
- [14] M. Ao and R. Walker, *CIOs' View of HIPAA Security Rule Implementation - An Application of Q-Methodology*, Journal of Healthcare Information Management **19**, 73 (2005).
- [15] R. Andis, *Noncompliant and Unconcerned*, Modern Healthcare **35**, 33 (2005).
- [16] A. Bourka, A. Kaliontzoglou, D. Polemi, A. Georgoulas, and P. Sklavos, *PKI-Based Security of Electronic Healthcare Documents*, in *SSGRR 2003w, International Conference on Advances in Infrastructure for Electronic Business, Science, Education, Medicine and Mobile Technology*, 2003.
- [17] D. Lorence and R. Churchill, *Incremental Adoption of Information Security in Healthcare Organisations: Implications for Document Management*, IEEE Transactions on Information Technology in Biomedicine **9**, 169 (2005).
- [18] V. Cheng and P. Hung, *Towards an Integrated Privacy Framework for HIPAA-Compliant Web Services*, in *CEC05: Proceedings of the Seventh IEEE International Conference on E-Commerce Technology*, pages 480–483, IEEE Computer Society, 2005.

- [19] J. S. Hooda, E. Dogdu, and R. Sunderraman, *Health Level-7 Compliant Clinical Patient Records System*, in *SAC '04: Proceedings of the 2004 ACM Symposium on Applied Computing*, pages 259–263, New York, NY, USA, 2004, ACM Press.
- [20] S. Gritzalis, C. Lambrinouidakis, D. Lekkas, and S. Deftereos, *Technical Guidelines for Enhancing Privacy and Data Protection in Modern Electronic Medical Environments*, *IEEE Transactions on Information Technology in Biomedicine* **9**, 413 (2005).
- [21] I. S. Organization, *ISO/DIS 27799 - Health informatics Security management in health using ISO/IEC 17799*, 2006.
- [22] Wikipedia, *Enterprise Information System — Wikipedia, The Free Encyclopedia*, 2004, [Online; accessed 22-July-2006].
- [23] Anonymous, *Soel Knowledge Documentation*, Software of Excellence Ltd., 2005, Unpublished User Manual.
- [24] United States Department of Health and Human Services, *Health Insurance Reform: Standards for Electronic Transactions; Announcement of Designated Standard Maintenance Organizations; Final Rule and Notice, 45 CFR Parts 160 and 162*, 2002.
- [25] C. McDonald, J. Overhage, M. Barnes, G. Schadow, L. Blevins, and P. Dexter, *The Indiana Network For Patient Care: A Working Local Health Information Infrastructure*, *Health Affairs* **24**, 1214 (2005).
- [26] B. Nuseibeh and S. Easterbrook, *Requirements Engineering: A Roadmap*, in *ICSE '00: Proceedings of the Conference on the Future of Software Engineering*, pages 35–46, New York, NY, USA, 2000, ACM Press.
- [27] P. Zave, *Classification of Research Efforts in Requirements Engineering*, *ACM Computing Surveys (CSUR)* **29**, 315 (1997).
- [28] J. Goguem and C. Linde, *Techniques for Requirements Elicitation*, in *Proceedings of the First International Symposium on Requirements Engineering*, pages 152–164, Los Alamitos, CA, 1993, IEEE Computer Society Press.

- [29] J. M. Moore and F. M. S. III, *A Comparison of Questionnaire-Based and GUI-Based Requirements Gathering*, in *ASE '00: Proceedings of the 15th IEEE International Conference on Automated Software Engineering*, page 35, 2000.
- [30] D. Hamilton, R. Covington, and J. Kelly, *Experiences in Applying Formal Methods to the Analysis of Software and System Requirements*, in *WIFT 5, Proceedings of IEEE Workshop Industrial-Strength Formal Specification Techniques*, 1995.
- [31] S. Easterbrook, R. Lutz, R. Covington, J. Kelly, Y. Ampo, and D. Hamilton, *Experience Using Lightweight Formal Methods for Requirements Modeling*, *IEEE Transactions on Software Engineering* **24**, 4 (1998).
- [32] A. van Lamsweerde, R. Darimont, and P. Massonet, *Goal Directed Elaboration of Requirements for a Meeting Scheduler: Problems and Lessons Learnt*, in *Proceedings of the 2nd IEEE International Symposium on Requirements Engineering*, pages 194–203, IEEE Press, 1995.
- [33] E. Letier and A. van Lamsweerde, *Deriving Operational Software Specifications from System Goals*, in *SIGSOFT '02/FSE-10: Proceedings of the 10th ACM SIGSOFT Symposium on Foundations of Software Engineering*, pages 119–128, New York, NY, USA, 2002, ACM Press.
- [34] A. Sutcliffe, *Scenario-Based Requirement Analysis*, *Requirements Engineering Journal* **3**, 48 (1998).
- [35] A. Silva, *Requirements, Domain and Specifications: A Viewpoint-Based Approach to Requirements Engineering*, in *ICSE '02: Proceedings of the 24th International Conference on Software Engineering*, pages 94–104, New York, NY, USA, 2002, ACM Press.
- [36] D. G. Firesmith, *Security Use Cases*, *Journal of Object Technology* **2**, 53 (2003).
- [37] D. Firesmith, *Specifying Reusable Security Requirements*, *Journal of Object Technology* **3**, 61 (2004).

- [38] N. R. Mead and T. Stehney, *Security Quality Requirements Engineering (SQUARE) Methodology*, in *SESS '05: Proceedings of the 2005 Workshop on Software Engineering for Secure Systems - Building Trustworthy Applications*, pages 1–7, New York, NY, USA, 2005, ACM Press.
- [39] J. D. Meier, A. Mackman, B. Wastell, P. Bansode, J. Taylor, and R. Araujp, *Security Engineering Explained*, Technical report, Microsoft Corporation, 2005.
- [40] S. Myagmar, A. Lee, and W. Yurcik, *Threat Modeling as a Basis for Security Requirements*, 2005.
- [41] I. Alexander, *Misuse Cases: Use Cases with Hostile Intent*, IEEE Software **20**, 58 (2003).
- [42] P. Hope, G. McGraw, and A. I. Antón, *Misuse and Abuse Cases: Getting Past the Positive*, IEEE Security and Privacy **2**, 90 (2004).
- [43] B. Schneier, *Modeling security threats*, Dr. Dobb's Journal (1999).
- [44] M. V. Higuero, J. J. Unzilla, E. Jacob, P. Saiz, M. Aguado, and D. Luengo, *Application of 'Attack Trees' in Security Analysis of Digital Contents E-Commerce Protocols with Copyright Protection*, in *CCST '05. 39th Annual 2005 International Carnahan Conference on Security Technology, 2005*, pages 57–60, IEEE Press, 2005.
- [45] C. Fung, Y. Chen, X. Wang, J. Lee, R. Tarquini, M. Anderson, and R. Linger, *Survivability Analysis of Distributed Systems Using Attack Tree Methodology*, in *Military Communications Conference, 2005. MILCOM 2005*, pages 1–7, IEEE Press, 2005.
- [46] Wikipedia, *Statistical Power — Wikipedia, The Free Encyclopedia*, 2006, [Online; accessed 8-September-2006].
- [47] K. Alderson, *Nurse Sacked for Altering Records After Baby's Death*, The Times (1995).

- [48] A. Podgurski and B. Kiraly, *Security Vulnerabilities and Conflicts of Interest in the Provider-Clearinghouse\*-Payer Model*, in *PORTIA Workshop on Sensitive Data in Medical, Financial, and Content-Distribution Systems*, Stanford CA, USA, 2004.
- [49] D. Russel and G. T. G. Sr., *Computer Security Basics*, O'Reilly Associates Inc., 1991.
- [50] B. Lampson, *Computer Security in the Real World*, *Computer* **37**, 37 (2004).
- [51] R. Sandhu and P. Samarati, *Authentication, Access Control, and Audit*, *ACM Computing Surveys (CSUR)* **28**, 241 (1996).
- [52] X. Chen, J. Zhang, D. Wu, and R. Han, *HIPPA's Compliant Auditing System for Medical Imaging System*, in *Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference*, pages 562–563, 2005.
- [53] S. Axelsson, *Intrusion Detection Systems: A Survey and Taxonomy*, Technical Report 99-15, Chalmers University, 2000.
- [54] J. N. Security and P. C. (SPC), *Security and Privacy Auditing in Health Care Information Technology*, Technical report, Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC), 2001.
- [55] G. Marshall and G. Dickinson, *Common Audit Message*, Technical report, HL7 Security and Accountability Special Interest Group, 2001.
- [56] HIMMS/RSNA, *IHE Technical Framework, Volume III*, 2002.
- [57] A. International, *E2147-01 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems*, 2002.
- [58] G. Marshall, *Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications*, Technical report, The Internet Society, 2004.
- [59] R. Allen, *Workflow: An Introduction*, Technical report, Open Image Systems Inc., United Kingdom. Chair, WfMC External Relations Committee.

- 
- [60] W. M. Coalition, *Interface 1: Process Definition Interchange (TC-1016)*, Technical report, WfMC: Brussels, 1996.
- [61] S. Graber, *The Impact of Workflow Management Systems on the Design of Hospital Information Systems*, in *Proceedings of AMIA Annual Fall Symposium*, pages 856–860, 1997.
- [62] P. Dadam, M. Reichert, and K. Kuhn, *Clinical Workflows – The Killer Application for Process-Oriented Information Systems?*, in *Proceedings of the 4 International Conference on Business Information Systems (BIS'2000)*, pages 36–59, 2000.