



## A Survey-Based Analysis of HIPAA Security Requirements

---

By Prof Clark Thomborson & Jinho Lee  
The University of Auckland



## Introduction

---

- In the US, HIPAA was passed to make adequate protection of e-PHI a legal requirement for the covered entities.
- Its provisions lack specificity with regard to threat model and architectural / implementation-level guidelines.
- A local software exporter 'Software of Excellence Ltd' expressed their difficulty in meeting the customers' varying security requirements.



## Objective

---

- To find out about the security concerns held by the US dental schools and use them to engineer specific security requirements.



## Methodology - Overview

---

- We used an online survey to obtain information from the US dental schools.
- With the help of Dr Gary Guest at the University of Texas Dental School, we designed the survey instrument and sent invitation letters through the American Dental Education Association (ADEA).



## Methodology – Survey Design 1

---

- We reviewed the existing requirement engineering methodologies.
  - Goal-based (e.g. Inquiry Cycle, KAOS)
  - Scenario-based (e.g. misuse case analysis)
  - Viewpoint-based (e.g. VBRE)
  
- We chose scenario-based methodology for our study and designed the survey accordingly to gather misuse cases from the participants.
  
- We hypothesised that our survey-based approach can discover more specific security requirements than the HIPAA provisions.



## Methodology – Survey Design 2

---

- Survey was structured according to the five standards in the Technical Safeguards of the HIPAA Security Rule
  - Access Control – who can access what
  - Audit Control – detecting misuses
  - Integrity – unauthorised alteration
  - Transmission Security – protecting while in transit
  - Entity Authentication – verifying entities



## Methodology - Survey Questions 1

---

- General Questions – To discover general perception of the respondents.
  - E.g. “Do you consider insider attacks as significant threats? If yes, please describe a scenario of a likely insider attack that you are concerned about”



## Methodology - Survey Questions 2

---

- Specific questions for each **standard** in the HIPAA Technical Safeguards.
  - **Type-1** “Are you satisfied with your current information system with respect to **Integrity**? If not, please describe why”
  - **Type-2** “Please describe a scenario of system use that you perceive as non-HIPAA compliant with regard to **Integrity**”



## Results - General

---

- Out of the 56 potential respondents we received 7 responses. 12.5% response rate.
- Among the five standards of the HIPAA Security Rule, the respondents were most concerned about 'Audit Control'.
- Insider attacks were considered to be significant threats.



## Results – Misuse Cases

---

- Four misuse cases were identified from the survey responses
  - Password sharing by legitimate insiders
  - Dentists covering up for dental malpractice
  - Email used by insiders to communicate e-PHI
  - Unauthorised access through workstations unattended by insiders



## Discussion

---

- Our finding that the dental schools' biggest concern with regard to HIPAA is the 'audit controls' standard agrees with Goedert's finding in 2005.
- Our result agrees with other works that claim insider attacks to be the greatest threat to system security
- All of the misuse cases identified from our survey were insider threats that required little technical sophistication. Similar finding in the financial sector.
- We believe our experimental hypothesis was confirmed - we successfully elicited some specific misuse cases.



## Questions??

---