



HIPAA And The Suitability of CRAMM

SIEMENS

Global network of innovation

Insight Consulting

Management in Confidence

TABLE OF CONTENTS

| | | |
|-----------|--|----------|
| 1. | INTRODUCTION..... | 1 |
| 2. | WHAT IS HIPAA ?..... | 1 |
| 3. | WHAT HIPAA INVOLVES | 1 |
| 4. | THE HIPAA SAFEGUARDS FRAMEWORK..... | 1 |
| 4.1. | HIPAA & RISK..... | 2 |
| 4.2. | HIPAA & ACCREDITATION OR CERTIFICATION | 2 |
| 4.3. | BS 7799 & ISO/IEC 17799 | 2 |
| 5. | SUMMARY OF CRAMM..... | 3 |
| 6. | USING CRAMM ON HIPAA PROJECTS | 4 |
| 7. | HIPAA SAFEGUARDS..... | 4 |

1. INTRODUCTION

This briefing note has been compiled to demonstrate CRAMM's capabilities and constraints in supporting the achievement of HIPAA compliance.

2. WHAT IS HIPAA ?

'HIPAA' is the 'Health Insurance Portability and Accountability Act' passed in the USA to ensure that customers are able to switch between health insurance providers as smoothly as possible without the unavailability, total loss or loss of integrity within their health data.

In order for USA-based organisations ('Covered Entities' - CEs) to comply with HIPAA requirements, they are required to demonstrate their ability to ensure the "Privacy of Individually Identifiable Health Information".

3. WHAT HIPAA INVOLVES

The activities required to comply with HIPAA are:

- ◆ **Initiation of a Project** within the organisation, suitably resourced in both financial terms and in terms of appropriately experienced personnel;
- ◆ Carry out a '**Baseline Assessment**' of the organisation to identify areas of compliance and non-compliance;
- ◆ Identify requirements for **Remedial Action**;
- ◆ Initiate a **Remedial Action Implementation** programme;
- ◆ **Validate Compliance**;
- ◆ **Maintain Compliance**.

However, as part of the Remedial Action Planning, there is a requirement to conduct a risk assessment and implement a risk management programme, which in turn has to an ongoing programme of review and improvement.

4. THE HIPAA SAFEGUARDS FRAMEWORK

These are provided in detail within the Security Standards annexes of the Act and are summarised in Appendix A to Sub-part C of Part 164.

They cover the following aspects:

- ◆ Administrative Safeguards;
- ◆ Physical Safeguards;
- ◆ Technical Safeguards.

These safeguards are attached and analyzed at the end of this paper.

Within each of the above sections, there are a number of subsections, which have specific requirements to be assessed, some of which are 'Required' (Baseline / Mandatory controls) and others that are designated 'Addressable' (Optional Controls).

4.1. HIPAA & RISK

Risk is typically the basis recommended for ensuring that IT systems handling, storing, manipulating and transmitting essential or critical data are appropriately protected. This too is the common ground with Corporate Governance, for which HIPAA can be depicted as the USA's 'Healthcare Information Governance' component, sitting alongside / overlapping with the Clinical Governance agenda.

In the UK, the NHS has adopted the Australian / New Zealand Risk Management Standard AS/NS 4360 for this area and has adopted CRAMM as its preferred method for InfoSec risk analysis and management.

It is Insight's understanding that those safeguards designated as 'Addressable' are required to be reviewed by means of the embedded Risk Assessment process. HIPAA, when defining Risk Assessment, does not mandate any particular method or process. However, it does state that the losses have to be determined assuming that there are no safeguards in place and that an assessment of threat and vulnerability should be performed.

Based on the results of the risk assessment, a decision is taken to determine whether the impact warrants the implementation of appropriate controls or countermeasures to 'address' the level of risk.

However, the Act specifies that if a CE chooses not to apply an Addressable control, then a risk acceptance statement of 'why not ?' is required to show that an objective process has been performed and a satisfactory level of risk acceptance has been adopted.

4.2. HIPAA & ACCREDITATION OR CERTIFICATION

A final requirement is for the CE to undertake Certification and Accreditation. This can be done either internally or externally. The implicit expectation of the Act is that the Certification or Accreditation of the Management System is of a working / established system rather than a newly created system ready to be implemented.

4.3. BS 7799 & ISO/IEC 17799

BS 7799 contains 2 components or parts. Part 1 provides a list of controls / safeguards that are accepted good practice. This part has also been adopted as ISO/IEC 17799. Part 2 of the standard provides a process and model for an Information Security Management System (ISMS) founded upon effective an effective, on-going, risk analysis and management process.

Certification is available against part 2 with about 120 organisations holding such status, although c.60% is presently UK based. BS 7799 Part 2 does not currently have an ISO equivalent but ratification of Part 2 as either ISO/IEC 17799 Part 2 or as ISO/IEC 27799 is expected shortly. Adoption of this

standard is growing internationally, including in the USA through Global Organisations, in part no doubt driven by HIPAA & GLBA requirements.

5. SUMMARY OF CRAMM

The CRAMM Version 5 'Expert' Toolkit, released in January 2003, is a comprehensive Information Security Support Tool and data repository that is presently in use in over 600 locations for over 430 organisations in 24 countries and 21 business sectors.

It has been used extensively within the UK National Health Service (NHS) to manage the risks to healthcare information and to support the achievement of the Information Governance goals of Patient Privacy, Data Protection, Freedom of Information, Data Quality and Security. The NHS has also used it to develop specific Risk Models to ensure that all NHS entities both meet a common minimum standard and achieve reasonable compliance against the requirements of BS 7799. The toolkit provides the following integrated functionality:

- ◆ For BS 7799 compliance or certification:
 - ◆ Initiation and scoping of compliance;
 - ◆ Gap Analysis (consistent with HIPAA's 'Baseline Assessment');
 - ◆ Action Planning (consistent with HIPAA's 'Remedial Action');
 - ◆ Security Improvement Programme (consistent with HIPAA's 'Remedial Action Implementation');
 - ◆ Statement of Applicability (providing a summary of the current compliance level);
 - ◆ Treatment of control Objective Reporting;
 - ◆ Compliance Checking (consistent with HIPAA's 'Validate Compliance');
 - ◆ Risk re-assessment (consistent with HIPAA's 'Maintain Compliance').
- ◆ For Information Security Risk Assessment;
 - ◆ Asset Identification;
 - ◆ Dependency Modelling;
 - ◆ Business Impact Assessment;
 - ◆ Threat and Vulnerability Assessment;
 - ◆ Calculation of Measures of Risk;
 - ◆ Calculation of Justified and Appropriate Countermeasures;
 - ◆ Countermeasure Gap Analysis including status reporting based upon management decisions for which supporting justifications can be collected;
 - ◆ Risk Management Decision Support;
 - ◆ Risk Treatment Reporting;
 - ◆ 'What If ?' Support.
- ◆ For Information Security Management;
 - ◆ Recovery Requirements Reporting;
 - ◆ Security Documentation 'Wizards';
 - ◆ Functionality to support Outsourcing;
 - ◆ Functionality to support Business Continuity Management Strategy Development.

In addition to handling financial impacts, CRAMM's Business Impact Assessment, being qualitative, also handles 'soft impacts', such as reputational loss, embarrassment, personal safety (i.e. loss of life) and legal breach etc. in a consistent manner.

CRAMM's threat and vulnerability assessment addresses all known threats to IT systems of all types whether technical, physical, logical, human or communications and can support the assessments with detailed questionnaires or user-entered opinions.

As can be seen on the safeguards tables below, the CRAMM Countermeasure Library covers all of the safeguards required by HIPAA and many more that HIPAA has overlooked.

6. USING CRAMM ON HIPAA PROJECTS

The stark and strong conclusion can be made that HIPAA compliance or certification can successfully and comprehensively be delivered by application of the BS 7799 ISMS Model and supporting processes.

In turn therefore, it can be equally strongly asserted that the adoption of CRAMM Version 5 is appropriate for HIPAA, fully supporting as it does both the BS 7799 and HIPAA Process models and key concepts.

7. HIPAA SAFEGUARDS

| Administrative Safeguards | | |
|----------------------------------|--|---|
| Safeguard | Aspect | Comment |
| Security Management Process | Risk Analysis (R) ¹ | Structured, consistent and reusable |
| | Risk Management (R) | In-built capability within the Toolkit |
| | Sanction Policy (R) | Addressed as part of the Countermeasure database ² |
| Assigned Security Responsibility | Information System Activity Review (R) | Addressed as part of the Countermeasure database |
| | (R) | Addressed as part of the Countermeasure database |
| Workforce Security | Authorisation/ Supervision (A) | Addressed as part of the Countermeasure database |
| | Workforce Clearance Procedure (A) | Addressed as part of the Countermeasure database |
| | Termination Procedure (A) | Addressed as part of the Countermeasure database |
| Information Access Management | Isolating Healthcare Clearinghouse functions (R) | Addressed as part of the Countermeasure database |
| | Access Authorisation (A) | Addressed as part of the Countermeasure database |
| Security Awareness & | Security Reminders (A) | Addressed as part of the Countermeasure |

¹ (R) = Required; (A) = Addressable

² This means that there are controls within the countermeasure database that will provide varying degrees of strength depending on the assessed level of risk (i.e. result of the risk assessment process)

Management in Confidence

| Administrative Safeguards | | |
|---|---|--|
| Training | | database |
| | Protection from Malicious Software (A) | Addressed as part of the Countermeasure database |
| | Log-in Monitoring (A) | Addressed as part of the Countermeasure database |
| | Password Management (A) | Addressed as part of the Countermeasure database |
| Security Incident Procedures | Response & Reporting (R) | Addressed as part of the Countermeasure database |
| Contingency Plan | Data Backup Plan (R) | Addressed as part of the Countermeasure database |
| | Disaster Recovery Plan (R) | Addressed as part of the Countermeasure database |
| | Emergency Mode Operation Plan (R) | Addressed as part of the Countermeasure database |
| | Testing & Revision Procedure (A) | Addressed as part of the Countermeasure database |
| Evaluation | (R) | Addressed as part of the Countermeasure database |
| Business Associate Contracts & Other Arrangements | Written contract or other arrangement (R) | Addressed as part of the Countermeasure database |

| Physical Safeguards | | |
|----------------------------|--|--|
| Safeguard | Aspect | Comment |
| Facility Access Controls | Contingency Operations (A) | Addressed as part of the Countermeasure database |
| | Facility Security Plan (A) | Addressed as part of the Countermeasure database |
| | Access Control & Validation Procedures (A) | Addressed as part of the Countermeasure database |
| | Maintenance Records (A) | Partially addressed as part of the Countermeasure database |
| Workstation Use | (R) | Addressed as part of the Countermeasure database |
| Workstation Security | (R) | Addressed as part of the Countermeasure database |
| Device & Media Controls | Disposal (R) | Addressed as part of the Countermeasure database |
| | Media Re-use (R) | Addressed as part of the Countermeasure database |
| | Accountability (A) | Addressed as part of the Countermeasure database |
| | Data Backup & Storage (A) | Addressed as part of the Countermeasure database |

| Technical Safeguards | | |
|---------------------------------|---|--|
| Safeguard | Aspect | Comment |
| Access Control | Unique User Identification (R) | Addressed as part of the Countermeasure database |
| | Emergency Access Procedure (R) | Partially addressed as part of the Countermeasure database |
| | Automatic Logoff (A) | Addressed as part of the Countermeasure database |
| | Encryption & Decryption (A) | Addressed as part of the Countermeasure database |
| Audit Controls | (R) | Addressed as part of the Countermeasure database |
| Integrity | Mechanism to Authenticate Electronic Protected Health Information (A) | Addressed as part of the Countermeasure database |
| Person or Entity Authentication | (R) | Addressed as part of the Countermeasure database |
| Transmission Security | Integrity Controls (A) | Addressed as part of the Countermeasure database |
| | Encryption (A) | Addressed as part of the Countermeasure database |