



# UNIVERSITY OF PLYMOUTH

MATURITY MODEL FOR HEALTHCARE CLOUD SECURITY

by

OPEOLUWA ORE AKINSANYA

A thesis submitted to the University of Plymouth

in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Engineering, Computing and Mathematics

July 2019

### **Copyright Statement**

This copy of the thesis has been supplied on condition that anyone who consults it is understood to recognise that its copyright rests with its author and that no quotation from the thesis and no information derived from it may be published without the author's prior consent.

## **Acknowledgements**

Firstly, my utmost appreciation is to Almighty God for the good and successful completion of my PhD.

I would like to express my heartfelt gratitude to my parents, my mother Modupeore, and my father Olukayode, for their support throughout this journey, which enabled me to reach this stage successfully. My greatest indebtedness goes to my husband Akinbolu, for his support, patience, prayers and encouragement, which were positive influences on me to complete this thesis. In addition, I owe special thanks to my father-in-law, Folarin, my siblings, Elisha, Olubunmi, Yosolu, David, Anu, Kunmi, Dara, Amina, Micheal, Iyanu, Elias, Eyinojuoluwa, Damiloju, and my close friends, from the Redeemer Church, and the Agboola's, for their moral support, endless patience and continuous prayers. This PhD work would not have been possible without the guidance and untiring support of my supervisory team, Dr. Maria Papadaki and Dr Lingfen Sun. Thanks to them for their timely and motivating advice throughout the PhD process.

Thanks must also go to the Centre for Security, Communications and Network Research (CSCAN) at University of Plymouth for providing a congenial and pleasant research atmosphere. Thanks also go to my fellow researchers within the CSCAN group for their support and interesting discussions. Lastly, I would like to express my thanks to all the experts for their participation in the survey; they supported my work in this way and helped me to achieve results of better quality.

### **Author's Declaration**

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Doctoral College Quality Sub-Committee. Work submitted for this research degree at the University of Plymouth has not formed part of any other degree either at the University of Plymouth or at another establishment.

Relevant seminars and conferences were regularly attended at which work was often presented and several papers were published in the course of this research project.

Word count of main body of thesis: 35469

Signed: \_\_\_\_\_

Date: 20/08/2019

### **List of Publications**

Akinsanya, O., Papadaki, M. and Sun, L., 2019. Towards a maturity model for health-care cloud security (M2HCS). *Information & Computer Security*, [online] ahead-of-print (ahead-of-print). DOI: <https://doi.org/10.1108/ICS-05-2019-0060>.

Akinsanya, O., Papadaki, M. and Sun, L., 2019. Factors Limiting the Adoption of Cloud Computing in Teleradiology. *International Journal for Information Security Research*, 9(2), pp.854-861. DOI: 10.20533/ijisr.2042.4639.2019.0098.

### **List of Presentation**

Balogun, O. and Papadaki, M., 2018. Organizational Factors Influencing Medical Data Sharing in Cloud. In: *International Conference for Internet Technology and Secured Transactions (ICITST)*. [online] Cambridge, UK: Infonomics Society, pp.184-187. Available at: <<https://www.orpems.org/Proceedings/ICITST-WorldCIS-WCST-WCICSS-2018-Proceedings.pdf>>.

Akinsanya, O., Papadaki, M. and Sun, L., 2019. Current Cybersecurity Maturity Models: How Effective in Healthcare Cloud?. In: *5th Collaborative European Research Conference (CERC)*. [online] Darmstadt, Germany: CEUR-WS.ORG, pp.211-222. Available at: <<http://ceur-ws.org/Vol-2348/paper16.pdf>>.

## **Abstract**

### **Maturity Model for Healthcare Cloud Security**

**Opeoluwa Ore Akinsanya**

Management of security across eHealth cloud services is a major organizational challenge that healthcare organizations seek to resolve in order to aid their trusts in cloud and increase the adoption of cloud services in healthcare. The organizational challenges regarding implementations of technical security solutions are the major limiting factors for the adoption of the eHealth cloud. As such, the aim of this research will focus on developing a security maturity model, which will help healthcare organizations to provide a description of the application of their cloud security services, and an assessment and improvement of their cloud security services over time, as well as to guide and educate relevant stakeholders concerning the optimization of their security practices. The identified gaps in the review are in the aspect of adoption – the maturity models are either too complicated to implement, or they require the healthcare organization's processes to be refined to suit the maturity model's implementation. The Maturity Model for Healthcare Cloud Security (M<sup>2</sup>HCS) was developed using the Design Science Research Methodology (DSRM). It was validated using a formulated case study, web-based survey and interviews with practitioners, DSRM framework, and feedback from scientific community. The novel contribution of this research is the proposal of the model. M<sup>2</sup>HCS is a high level, holistic model that can be used to support and promote healthcare organization's usable security practices against cyber and cloud security attacks.

## Table of Contents

Copyright Statement .....	1
Acknowledgements .....	2
Author's Declaration .....	3
Abstract .....	4
Table of Contents .....	6
List of Tables .....	12
List of Figures .....	13
List of Equations .....	14
Chapter One .....	15
1 Introduction .....	15
1.1 Problem Statement .....	16
1.2 Research Question .....	17
1.3 Research Aim and Objectives.....	17
1.4 Research Methodology .....	18
1.5 Thesis Structure.....	20
1.6 Conclusion.....	21
Chapter Two .....	22
2 Cloud-Based Healthcare in Europe .....	22
2.1 Health Records on the Cloud.....	23
2.2 eHealthcare Cloud Projects in Europe.....	26
2.2.1 Model-Driven European Paediatric Digital Repository (MD-Paedegree) ..	26

2.2.2	Simulation Modelling of Coronary ARtery Disease: A Tool for Clinical Decision Support (SMARTool).....	29
2.2.3	Electronic Health Records for Clinical Research (EHR4CR) .....	32
2.3	Challenges Limiting eHealth Cloud Adoption.....	34
2.4	Conclusion .....	37
Chapter Three.....		38
3	Assessing Challenges in Adoption of eHealth Cloud.....	38
3.1	Data Collection Process/Methodology .....	39
3.2	Background of Study Participants .....	40
3.3	Scope of Study .....	41
3.3.1	Study Question.....	42
3.3.2	Findings on the Factors Limiting Adoption of eHealth Cloud .....	43
3.3.2.1	Technical Challenges.....	43
3.3.2.1.1	Service Reliability and Availability .....	43
3.3.2.1.2	Web Performance and Latency .....	45
3.3.2.1.3	Disaster Recovery .....	45
3.3.2.1.4	Integration and Interoperability.....	47
3.3.2.1.5	Data Portability.....	49
3.3.2.1.6	Data Quality .....	49
3.3.2.1.7	Access Control Solutions for Clinical Workflow.....	50
3.3.2.2	Organisational Challenges .....	53
3.3.2.2.1	Financial Costs .....	54
3.3.2.2.2	Organisational Culture Changes .....	56
3.3.2.2.3	End Users' Assessment and Trust.....	57
3.3.2.3	Legal Challenges.....	59
3.3.2.3.1	Standards.....	60
3.3.2.3.2	Data Privacy Legislation .....	61
3.4	Influence of the Identified Challenges Limiting eHealth Cloud Adoption	



3.5	Chapter Conclusion .....	63
	Chapter Four.....	64
4	Theoretical Framework for Proposed Maturity Model.....	64
4.1	Systematic Literature Review .....	64
4.1.1	Systematic Literature Search Approach.....	64
4.2	Cloud Security .....	69
4.3	Cloud Security in Healthcare .....	71
4.4	Cyber Security Standards, Best Practices, and Guidance.....	77
4.4.1	International Organisation for Standardisation (ISO) .....	78
4.4.2	Health Information Trust Alliance Common Security Framework (HITRUST CSF) .....	80
4.4.3	National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).....	81
4.4.4	Health Insurance Portability and Accountability Act (HIPAA) .....	83
4.4.5	Cloud Security Alliance Standards Cloud Controls Matrix (CSA CCM).....	84
4.4.6	Summary of Reviewed Standards .....	85
4.5	Comparison of Maturity Models Applicable in Healthcare.....	87
4.5.1	Information Security Focus Area Maturity Model .....	89
4.5.2	Cloud Security Capability Maturity Model.....	90
4.5.3	NHS National Infrastructure Maturity Model .....	91
4.5.4	Health Information Network Capability Maturity Model .....	93
4.5.5	Summary and Analysis of Reviewed Maturity Models .....	94
4.6	Identified Research Gaps and Operational Characteristics of Proposed Model.....	98
4.7	Chapter Conclusion .....	101
	Chapter Five .....	103
5	Maturity Model Development.....	103

5.1	M <sup>2</sup> HCS Development Methodology .....	103
5.2	M <sup>2</sup> HCS Maturity Model .....	109
5.2.1	M <sup>2</sup> HCS Maturity Domains .....	110
5.2.2	M <sup>2</sup> HCS Maturity Levels .....	115
5.3	Metrics .....	122
5.3.1	M <sup>2</sup> HCS Metric .....	122
5.3.1.1	Decision Process for Assigning Maturity Level .....	124
5.3.1.2	How to Measure .....	127
5.3.2	Assessment Using Adopted Healthcare Domain-Specific Metrics.....	128
5.4	Senior Management Support .....	132
5.5	Chapter Conclusion .....	132
Chapter Six .....		134
6	Validation of Maturity Model for Healthcare Cloud Security.....	134
6.1	Validation Strategy.....	134
6.2	Survey and Interview .....	135
6.2.1	Background of Study Participants .....	136
6.2.2	Survey and Interview Protocol .....	140
6.2.3	Survey and Interview Results .....	142
6.2.3.1	Maturity Model Validation Feedback .....	142
6.2.3.2	Domain, Maturity Levels, Objectives Validation Feedback .....	144
6.2.4	Influence of Feedback on Proposed Maturity Model .....	146
6.3	Proposed Maturity Model Changes and Improvements .....	148
6.3.1	Framework Refinement .....	149
6.4	Practical Validation of the Research Findings.....	153
6.4.1	Demonstration of Case Study Stage .....	154
6.4.2	Case Study .....	155
6.4.3	Case Study Assessment .....	161

6.4.4	Improving Maturity .....	164
6.4.5	Presentation of the M <sup>2</sup> HCS Framework Prototype.....	165
6.5	Academic Peer Review.....	169
6.6	Limitations of the Study .....	170
6.7	Chapter Conclusion .....	171
Chapter Seven.....		172
7	Research Overview .....	172
7.1	Communication.....	174
7.2	Research Contributions and Findings.....	174
7.3	Research Limitations .....	180
7.4	Recommendations for Further Research.....	181
7.5	Conclusion.....	183
Appendices .....		184
Appendix A1 - M <sup>2</sup> HCS detailed matrix (IAM) .....		184
Appendix A2 - M <sup>2</sup> HCS detailed matrix (IRM) .....		188
Appendix A3 - M <sup>2</sup> HCS detailed matrix (ERM).....		192
Appendix A4 - M <sup>2</sup> HCS detailed matrix (PeS).....		196
Appendix A5 - M <sup>2</sup> HCS detailed matrix (PhS) .....		200
Appendix B - Research Ethics .....		204
Appendix C - Survey Information Guide.....		206
Appendix D - Survey Questions.....		207
Appendix E - Interview Summary.....		220

Appendix F - Interview Question Guide .....	222
Bibliography .....	229
List of Publications .....	252

## **List of Tables**

Table 1.1 Relationship between the thesis chapters and the DSRM phases.....	21
Table 3.1 Data Collection Process.....	40
Table 4.1 Summary of reviewed standards.....	87
Table 4.2 Summary of reviewed maturity models .....	97
Table 5.1 Decisions taken for the design of M2HCS (Mettler and Rohner, 2009)M <sup>2</sup> HCS Development Process.....	108
Table 5.2 Dimensions of M2HCS.....	114
Table 5.3 Influences of Foundational Maturity Models and Development of Maturity Levels.....	117
Table 5.4 Summary of M2HCS Maturity Levels and Practises .....	117
Table 5.5 Elements of Security Posture (Jafari et al., 2010) .....	131
Table 6.1 Pre-Assessment Information about the Participants .....	137
Table 6.2 Summary of the Research Participants.....	139
Table 6.3 Scale Used in the Survey.....	142
Table 6.4 Maturity Model Validation Feedback .....	142
Table 6.5 Domain/Maturity Levels/Objectives Validation Feedback .....	145
Table 6.6 Survey Outcomes from Participants on Domains.....	146
Table 6.7 Refinement of M2HCS framework .....	152
Table 6.8 Maturity Ratings for Each Domain .....	162
Table 6.9 Research Outputs: External Validation .....	170

## List of Figures

Figure 1.1 Phases of DSRM (Peffer <i>et al.</i> , 2008) .....	20
Figure 4.1 Systematic Literature Search (Duff, 1996) .....	65
Figure 4.2 Search and Exclusion Process .....	68
Figure 5.1 Mettler Methodology Decision Parameters (Carvalho <i>et al.</i> , 2017) .....	104
Figure 5.2 Activities for the development of M2HCS.....	109
Figure 5.3 Influences of Foundational Models and Development of Maturity Domains.....	111
Figure 5.4 Detailed Dimensions of M2HCS .....	121
Figure 5.5 M2HCS Metrics Framework.....	126
Figure 6.1 Revised M2HCS .....	153
Figure 6.2 Screenshot of the Login Form.....	167
Figure 6.3 Sample of Assessment Process .....	167
Figure 6.4 Result Page of the Assessment.....	168
Figure 6.5 Previous Assessment Results .....	168

## List of Equations

Equation 1 M2HCS Formula .....	128
--------------------------------	-----

## **Chapter One**

### **1 Introduction**

An important aspect of increasing the adoption of cloud computing in healthcare is the comprehensive knowledge and operational implementation of security and privacy in eHealth cloud computing (Zhang and Liu, 2010). Notwithstanding the potential improvements from the implementation of eHealth cloud services, (information) security is still uncertain, and this issue is believed to be more complex regarding the cloud services (Almorsy, Grundy and Müller, 2010).

Cloud computing is a computing and communication model with the potential to revolutionise the way systems and services are considered (Mell and Grance, 2011). For eHealth, the advantages of using the cloud services are clear due to the prompt provisioning of computational resources and limited human administration effort or service provider interaction. For this reason, cloud computing services can deliver eHealth care services in diverse settings and with an operational and resourceful approach (Rodrigues *et al.*, 2013).

As further emphasised by the European Network and Information Security Agency (ENISA) in their reports (Catteddu and Hogben, 2009; Haeberlen, and Dupre, 2012), the cloud also presents the top security risks that currently characterize key limitations for its adoption. An essential aspect of healthcare that has improved over the past couple of decades is ensuring health information security and privacy, which is a constant process (Solove, 2013). Predominantly, it is the responsibility of the healthcare organisation to ensure and maintain the security of their healthcare information. Thus, essential developments and



methods for this must be scheduled and executed. This is especially vital whilst outsourcing computing services in a cloud to guarantee an applicable level of security.

In other critical infrastructure sectors such as energy (Christopher *et al.*, 2014) and financial services (Josh and DePierro, 2018), well-designed security metrics are valuable in not only facilitating the correct application of different security mechanisms provided by a system but also in recognising its weaknesses and evaluating the effectiveness of the diverse security mechanisms being executed. However, based on the limited adoption of cloud in the healthcare environment, there are a small number of research studies aimed at building a security model, or a matrix of a common set of security objectives, and quantitative security metrics for the eHealth cloud. To the researcher's knowledge, a particular maturity model for security administration in cloud computing for healthcare currently does not exist.

### **1.1 Problem Statement**

Security is one of the biggest issues in the general cloud computing field, particularly as it relates to healthcare. Most healthcare organisations view cloud computing suspiciously because of its probable security risks, which has in turn limited their adoption of cloud services (Kuo, 2011; AbuKhousa, Mohamed and Al-Jaroodi, 2012; Haufe, Dzombeta and Brandis, 2014; Mehraeen *et al.*, 2016; Subramanian and Jeyaraj, 2018).

Management of security across eHealth cloud services is a major organisational challenge that healthcare institutions seek to resolve to increase their trust in

cloud and their adoption of cloud services. A healthcare organisation's business strategy and goals must be developed and implemented in the context of security. Hence, the security risks relating to eHealth cloud must be identified, evaluated, and mitigated in the development process (Haeberlen and Dupre, 2012).

## **1.2 Research Question**

The significance of maintaining secure and trusted eHealth cloud services has resulted in a central question for this research:

How are the security practises of healthcare organisations actively using cloud services assessed?

To address this research question, this study proposes a novel maturity model for assessing security practises in healthcare organisations actively using cloud services.

## **1.3 Research Aim and Objectives**

The aim of this research is to develop a maturity model for eHealth cloud services that can be utilised to describe the application of security services and -an assessment of these services over time. It is also intended to guide and educate relevant stakeholders concerning the optimisation of security practises. To realise the research aim, the following objectives are developed:

- ⇒ Identify the major factors limiting the adoption of cloud services in healthcare.
- ⇒ Demonstrate the knowledge of cybersecurity standards and maturity models relevant to ensuring the security of eHealth cloud.
- ⇒ Develop a maturity model for healthcare cloud security.

- ⇒ Validate that the proposed model is applicable in the real healthcare environment.

## 1.4 Research Methodology

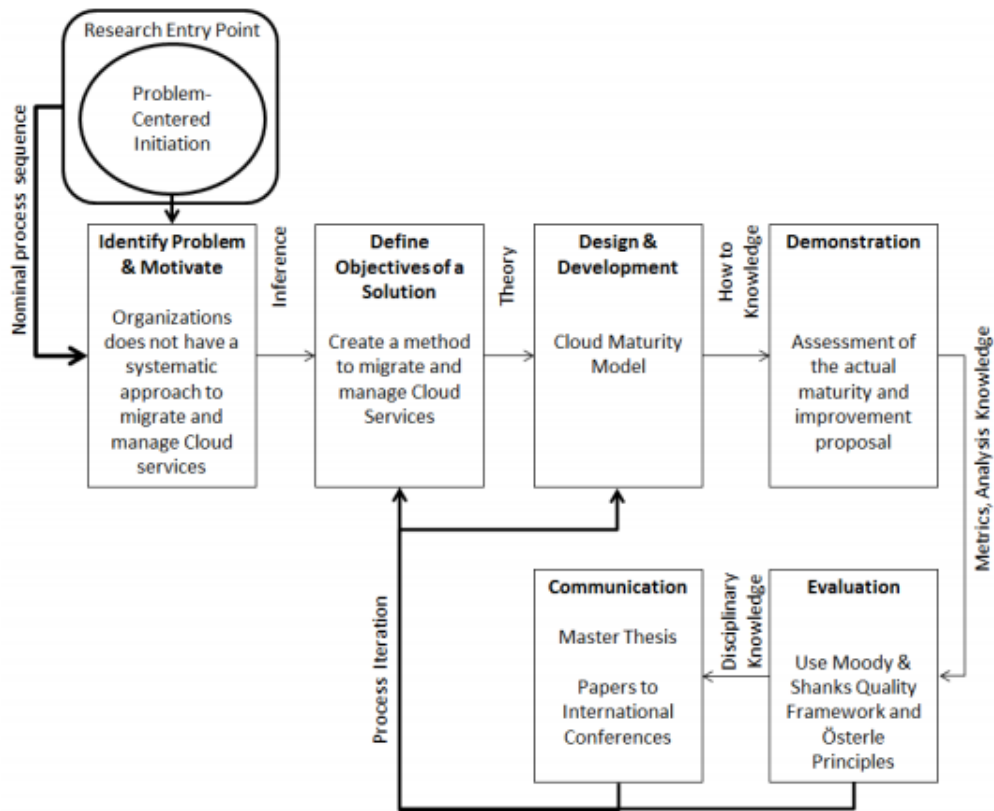
The Design Science Research Methodology (DSRM) has been adopted for this study. In DSRM, the concept of methodology is defined as ‘a system of principles, practices and procedures applied to a given branch of knowledge’ (Hevner *et al.*, 2004). Thus, this adopted methodology in the context of information systems involves the construction and assessment of a novel artefact that resolves a precise issue in a particular field (Hevner *et al.*, 2004). These artefacts comprise constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practises), and instantiations (implemented and prototype systems) (Hevner *et al.*, 2004). In this research, the proposed artefact is a model.

DSRM entails an iterative process composed of six steps (Figure 1.1) and includes rigorous approaches for the construction and assessment of the artefact. These phases are explained below:

- ⇒ Identification of the problem and research motivation: Describe the particular research problem and validate the significance of the solution. In this phase, it is essential to identify the state of the problem and to evidently validate the significance of the solution.
- ⇒ Define the solution’s objectives: Provide a description of the purposes of the solution and the state of the art, taking into account what is promising and realistic. The solution can be quantitative or qualitative.

- ⇒ Design and development: Construct the artefact, define its anticipated service, develop its design, and build the tangible artefact. The artefact can be a premeditated piece in which a research contribution is entrenched in the design.
- ⇒ Validation: This phase compares the proposed objectives of the solution to real practical results from the artefact in the demonstration. Well-implemented validation approaches are used to determine the effectiveness, quality, and ability of the planned artefact. The approaches include the use of a case study, web-based surveys, and interviews with relevant expert practitioners. After this step, researchers can decide if it is necessary to iterate back to improve the artefact.
- ⇒ Communication: This focusses on the communication of the research as a whole, consisting of the problem, objectives, artefact, demonstration, and validation, to appropriate audiences. The submission for publications and presentation of papers must be undertaken in this phase.

Even though DSRM is a sequential process, researchers do not have to chronologically proceed through each phase or commence at phase 1. Although not shown in Figure 1.1 there are several access points through which researchers can commence, such as problem identification and motivation, definition of the objectives of a solution, design and development, or demonstration.



**Figure 1.1 Phases of DSRM** (Peppers *et al.*, 2008)

## 1.5 Thesis Structure

This research adopts DSRM and is, therefore, organised in accordance with the phases recommended by this methodology. The relationship between the thesis chapters and the DSRM phases is presented in Table 1.1.

DSRM PHASES	THESIS CHAPTERS
Identification of problem and research motivation	Chapter 2—Factors limiting the adoption of cloud in healthcare
Definition of the solution's objectives	Chapter 3—Review of cybersecurity standards and maturity models
Design and development	Chapter 4—Proposed maturity model development
Demonstration	Chapter 5—Validation of the proposed maturity model, M <sup>2</sup> HCS
Validation	Chapter 5—Validation of the proposed maturity model, M <sup>2</sup> HCS
Communication	Chapter 6—Conclusions and future work

**Table 1.1 Relationship between the thesis chapters and the DSRM phases**

## **1.6 Conclusion**

The chapter presents the statement of problem, central question for the research, objectives developed to attain the aim of research. In conclusion, the phases involved in the chosen methodology, and structure of the thesis are discussed. The following chapter will seek to provide initial literature review by discussing about the cloud-based healthcare in Europe.

## Chapter Two

### 2 Cloud-Based Healthcare in Europe

Over the last years, health informatics has matured. The field is committed to improve quality in health care, provide best evidence at the point of need, and also demonstrate benefits across settings, taking advantage of technological opportunities and applications (Moen *et al.*, 2013). Technological and medical practitioners, publications, and social perspectives shows evidence of eHealth evolution but also point out significant eHealth concerns across Europe (Kummervold *et al.*, 2008). These concerns vary from the experiences of medical practitioners and patients working and living in technology-assisted environments (Moen *et al.*, 2011) and eHealth prospects to install, assess, and amend care services (Andersen *et al.*, 2008) to internationally oriented policies and programmes supporting patient safety (Nøhr & Aarts, 2010), interoperability for seamless care (Blobel, Hvannberg & Gunnarsdóttir, 2010), cross-border care (Stoicu-Tivadar *et al.*, 2011), and suitable business models for healthcare technologies (van Limburg *et al.*, 2011). In these areas, advances in eHealth can support future requirements within the healthcare system and improve the quality of life of citizens, patients and medical practitioners.

In Europe, the expressions ‘health informatics’, ‘medical informatics’, ‘nursing informatics’, and ‘radiology informatics’ are often used interchangeably with the term ‘eHealth’. eHealth can be defined in relation to its broader aim within the healthcare system (Eysenbach, 2001) to support medical practitioners in their work and continuous lifetime learning, in addition to helping citizens in their healthcare management. In addition, eHealth strives for reliable health

information (ignoring organisational boundaries) and functioning of healthcare systems. This description indicates the potentials of eHealth as a contributor to meet challenges for healthcare provisioning and improve healthcare systems across Europe (Stroetmann *et al.*, 2011). However, this does not reflect the eHealth solutions implemented on the cloud paradigm.

Relevant literature was reviewed and selected based on its contributions to eHealth project implementations and cloud adoption in healthcare with the objective of discussing the concept of cloud computing and presenting challenges to eHealth in Europe.

## **2.1 Health Records on the Cloud**

The secure exchange of Protected Health-related Information (PHI) such as healthcare examinations and reports has been an indispensable part of quality medical practise. The major reason for sharing PHI is to establish a longitudinal healthcare record for the patient through availability of historical examinations to compare with current examinations. Hence, a massive increase in healthcare records has resulted in a big challenge of data storage for healthcare providers as they must ensure excellent care services whilst reducing costs. In addition, increased movement of patients between doctors, healthcare organisations, and geographic locations has also created a problem in sharing PHI (Mendelson *et al.*, 2008; Flanders, 2009; Mendelson, Erickson and Choy, 2014).

Furthermore, the explosive growth in healthcare records is a result of the increasing age of the patient population, new medical technologies such as 3D imaging scans, and the increase in the size of patient data studies. Many



healthcare organisations do not have sustainable IT resources or storage for managing the increasing volume of patients' data.

Cost and security are the major evaluating factors for managing healthcare data storage and access (Shini, Thomas and Chithraranjan, 2012). As a result, healthcare-sharing media has evolved from the use of physical media such as hard copy documents to online platforms. However, the use of cloud computing for healthcare data sharing also has workflow-related and technical challenges, for which this research is a part of the solutions being developed (Mendelson, Erickson and Choy, 2014).

Prompt healthcare data sharing can increase the quality of healthcare. Furthermore, elimination of physical media reduces the chances of loss or corruption of healthcare data. Unnecessary healthcare costs based on duplicative examinations are also eradicated. Hence, these benefits of cloud-based healthcare data sharing are becoming clear to stakeholders across healthcare organisations (Flanagan *et al.*, 2012).

Lastly, eHealth cloud adopts a principle for healthcare data sharing called remote rendering, which ensures the actual healthcare data does not leave the secure server in the cloud. Hence, only HyperText Markup Language (HTML) pages of the data are downloaded to a healthcare practitioner's device, solving the problem of data incompatibility between multiple systems (Philbin, Prior and Nagy, 2011). Further illustrations are seen from the discussion of the related reviewed projects in section 2.2.

Cloud computing is a paradigm for storing and transmitting computing services and data over the Internet. It provides self-service access to scalable and shared

computing resources such as high computing power and massive storage space through communication networks. In addition, it provides an on-demand capacity to adjust resources as needed without human interaction. The eHealth cloud also provides large-scale data-oriented systems, which meet the needs for medical applications, as well as comprehensive access to PCs, networks, smartphones, and network-enabled medical devices (Lounis, 2014).

eHealth cloud can significantly support 'patient-centricity' in providing medical services. This trend has led to progress in adoption of Electronic Healthcare Records (EHR) that provide comprehensive care, patient security, point-of-care access to demographic and medical information, and clinical decision support. Availability of patients' data, regardless of the location of the patient and the medical practitioners, has become crucial to patient satisfaction and improved clinical results. Other primary benefits of e-Health cloud include:

⇒ Collaboration: Medical practitioners require team-based care delivery, a common set of clinical information, and ability to use applications based on business model requirements to perform their diagnoses and deliver appropriate care services. Cloud technologies support information synchronisation and sharing simultaneously. Amongst the early achievements of cloud-based collaboration solutions are remote video conference visits.

⇒ Clinical research aid: Pharmacology dealers are adopting cloud with the aim of lowering the cost and increasing the development of new drugs. The increasing significance of biologics in the research process is making cloud computing an increasingly important aspect of Research and

Development (R&D). Many pharmacology organisations do not presently have the ability to run large datasets, specifically DNA sequencing, as the data size overpowers their computers.

However, despite these benefits, using cloud to store medical data could imply moving patients' data from a trusted environment, such as a healthcare provider's infrastructure, to an untrusted environment such as cloud servers, which may be located outside the country and under different regulations (*Impact of Cloud Computing on Healthcare Version 2.0*, 2017).

Despite this risk, e-Health Cloud benefits are further discussed in relation to the Europe-based eHealthcare cloud projects reviewed below, as well as the benefits of adopting cloud in radiology.

## **2.2 eHealthcare Cloud Projects in Europe**

The European Union is leading the world in the development of new technology in healthcare, such as electronic patient records and telemedicine. However, there exist some practical obstacles to its wider use, according to a study conducted for the European Commission (Watson, 2010).

### **2.2.1 Model-Driven European Paediatric Digital Repository (MD-Paedigree)**

#### **Background of the Project**

The Model-Driven European Paediatric Digital Repository project has developed a digital repository to store paediatric clinical data for millions of young patients, enabling physicians to make more informed decisions. The advanced digital repository integrates data from clinical, genetic, and meta-genomic analyses, magnetic resonance image and ultrasound image analytics, haemodynamics,

real-time processing of musculoskeletal parameters, and fibres biomechanical data.

The platform provides decision support to medical professionals, wherever they treat their young patients, by looking for similarities amongst their own patients, accessing model-based simulations and predictions, and looking for patient-centric clinical workflows. It improves the diagnostic precision of paediatricians and offers child-specific treatment choices through disease simulations. It also employs cloud computing to meet the requirements of high performance and supercomputer resources.

MD-Paedigree is based on two previous, highly successful disease models, Health-e-Child (Freund *et al.*, 2006) and Sim-e-Child (Ionasec R., Suehling M. and Comaniciu D., 2010). However, it enhances these existing disease models by developing robust and reusable multiscale models for safer and more predictive, individualised, and effective healthcare in several disease areas. Furthermore, it builds on the eHealth platform already developed for Health-e-Child and Sim-e-Child to establish a worldwide advanced paediatric digital repository.

### **Aim of the Project**

The aim of MD-Paedigree is to reduce medical errors and suboptimal treatments, as well as decrease overall medical costs. It hosts data leveraged by advanced analytics tools such as deep machine learning or similarity search to identify hidden common patterns. From there, physicians can build personalised models to reproduce the individual patient's physiological parameters, either at a pre-interventional level or as a result of a given clinical intervention, and categorise

patients based on disease risk. Using these tools minimises the chance of medical error and increases treatment efficacy, reducing, in turn, the risks of complications and relapse, time of recovery, and clinical costs. MD-Paedigree's aims, therefore, are to:

- ⇒ integrate and share highly heterogeneous biomedical information, data, and knowledge, using best practises from the biomedical semantic web
- ⇒ develop holistic search strategies to seamlessly navigate through and manage the integrative model-driven info-structure and digital repository
- ⇒ jointly develop reusable, adaptable, and composable multiscale Virtual Physiological Human (VPH) workflow models
- ⇒ support evidence-based translational medicine at the point of care
- ⇒ facilitate collaborations within the VPH community (Athena, 2017)

### **Benefits and Challenges of the Project**

MD-Paedigree services a broad range of off-the-shelf models and simulations to support physicians and clinical researchers in their daily work. It vertically integrates data, information, and knowledge of incoming patients in participating hospitals across Europe and in the United States and provides innovative tools to define new workflows of models towards personalised predictive medicine. MD-Paedigree integrates methodological approaches from the targeted specialties and, consequently, analyses biomedical data derived from a multiplicity of heterogeneous sources, as well as specialised biomechanical and imaging simulation models (Pasche *et al.*, 2016).

It provides three fundamental functionalities in addition to those of an advanced electronic health records registry:

- ⇒ Similarity search, allowing clinicians to access ‘patients like mine’ (and find decision support for optimal treatment also based on comparative outcome analysis) and allowing patients to get in touch with ‘patients exactly like me’
- ⇒ Model-based patient-specific simulation and prediction
- ⇒ Patient-specific clinical workflows.

Using MD-Paedigree, doctors can select a highly individualised treatment option and receive on-the-spot support in predicting the likely outcome of such treatments based on each patient’s personal medical data. This leads to a future where child healthcare will become more effective, personalised, and affordable. At present, however, although the clinicians have largely recognised the added value of the implemented technological solutions, particularly for supporting their clinical decision making, the user interface has not yet reached the maturity level required for a seamless integration into everyday clinical practise.

## **2.2.2 Simulation Modelling of Coronary ARtery Disease: A Tool for Clinical Decision Support (SMARTool)**

### **Background of the Project**

SMARTool is a project aimed at developing IT solutions to support clinicians in the prevention and treatment of heart disease. In particular, the project involves the development of a platform to improve risk assessment in patients with coronary artery disease, such as myocardial infarction. It also develops

innovative IT solutions useful in the prevention and treatment of atherosclerosis-related diseases, a major cause of mortality and morbidity in all countries across the world.

SMARTool involves a software platform based on cloud computing technology for the development of computer models that, starting from non-invasive diagnostic imaging techniques, simulate the formation and growth over time of coronary plaque, fatty deposits responsible for the narrowing of the coronary arteries at the base of atherosclerosis. The platform is used with a perspective of personalised medicine; the predictive model adopted, in fact, is integrated with all clinical data of the individual patient including genetic factors, medical history, risk factors, and environmental factors. The solution is aimed at preventing the risk of certain acute complications of coronary artery disease (Parodi, 2016).

### **Aim of the Project**

SMARTool develops a Cloud-based Clinical Decision Support System (CDSS) for the prevention, management, and stratification of patients with Coronary Artery Disease (CAD), Coronary Heart Disease (CHD), and Major Adverse Cardiovascular Events (MACE). This is achieved through the standardisation and integration of heterogeneous health data and existing patient-/artery-specific multiscale and multilevel predictive models (Rocchiccioli *et al.*, 2017). Specifically, the SMARTool models are based on the extension of the already available multiscale and multilevel ARTreat models for coronary plaque assessment and progression over time using non-invasive imaging by Coronary Computed Tomography Angiography (CCTA) and are extended with functional site-specific assessment (hemodynamically significant plaque through non-

invasive Fractional Flow Reserve (FFR) computation) and additional heterogeneous patient-specific non-imaging data (history, lifestyle, exposure, bio-humoral data, phenotyping, and genotyping).

### **Benefits and Challenges of the Project**

SMARTool supports clinicians in the diagnosis, prognosis, and treatment of patients and optimisation of coronary revascularisation interventions with angioplasty and stent insertion. This provides cardiologists, hospitals, and clinical centres with an advanced tool for early diagnosis and disease risk assessment with the aim of improving, in particular, primary and secondary prevention as well as the treatment of acute events such as myocardial infarction (Sakellarios *et al.*, 2017).

SMARTool cloud-based platform provides as output a CDSS, assisted by a microfluidic device as a point-of-care testing of inflammatory markers for:

- ⇒ Patient-specific CAD stratification—Existing models, based on clinical risk factors, are implemented by patient genotyping and phenotyping to stratify patients with no obstructive CAD, obstructive CAD, and those without CAD.
- ⇒ Site-specific plaque progression prediction—Existing multiscale and multilevel ARTreat tools of CAD progression prediction are refined by genotyping and phenotyping parameters, tested by baseline, follow CCTA, and are integrated by non-imaging patient-specific data.



⇒ Patient-specific CAD diagnosis and treatment—Lifestyle changes, standard or high-intensity medical therapy, and a virtual angioplasty tool provide the optimal stent type(s) and site(s) for appropriate deployment.

### **2.2.3 Electronic Health Records for Clinical Research (EHR4CR)**

#### **Background of the Project**

The EHR4CR project involves a total of ten companies from the pharmaceutical industry, eleven university hospitals, and numerous academic groups and patient organisations. Together, the partners established a technical platform that makes it easier to link electronic health records to research platforms and networks in the healthcare sector. In doing so, a great deal of importance is being attached to data protection in particular; the platform is being created in such a way that analysis of the de-identified data takes place at an early stage in the relevant hospital. All disclosure of person-related data takes place only with explicit consent from the patient, who, as previously, is asked by his or her attending doctor whether he or she wishes to give his or her consent (Thorp *et al.*, 2015).

The project has developed a robust and scalable platform that can utilise de-identified data from hospital EHR systems. The EHR4CR platform supports distributed querying to assist in clinical trials' feasibility assessment and patient recruitment. The platform can connect securely to the data within multiple hospital EHR systems and clinical data warehouses across Europe to enable a trial sponsor to predict the number of eligible patients for a candidate clinical trial protocol, to assess its feasibility, and to locate the most relevant hospital sites. Applications for internal use are offered to connected hospitals to assist them

efficiently identify and contact the patients who may be eligible for particular clinical trials. Contrary to other initiatives, EHR4CR designed a solution which is compliant to EU legislation and respects the position of hospitals and patients. One of the key aspects is that patient-level data never leaves the connected hospitals (De Moor *et al.*, 2015).

### **Aim of the Project**

An aim of the EHR4CR project is to address the patient recruitment issues commonly facing clinical trials. Finding adequate numbers of eligible patients is often very difficult and always time consuming in a clinical trial project. The project aims to resolve such issues by integrating distributed hospital data resources and supporting automated queries. In principle, the enhanced availability of patient data will make patient discovery much easier and quicker. The EHR4CR services encompass:

- ⇒ clinical trial feasibility (distributed queries)
- ⇒ patient identification and recruitment (distributing trial protocols to sites and collecting follow-up information on recruitment status from sites)
- ⇒ clinical trial execution and serious adverse events reporting (mainly EHR extraction)

### **Benefits and Challenges of the Project**

EHR4CR has shown that it can significantly improve the efficiency of designing and conducting clinical trials, reducing time and costs, reducing administrative burdens, optimising protocol feasibility assessments, accelerating patient recruitment, making study conduct more efficient, and enabling the participation

of European hospitals in more clinical trials and thereby potentially increasing research income. The EHR4CR services will offer such benefits to hospitals as:

- ⇒ Enhancing the quality of patient-level EHR data for clinical research and improving quality of care and health outcomes
- ⇒ Generating a new additional income stream by contributing EHR data to research
- ⇒ Conducting clinical trials more efficiently and increasing hospital participation in a larger number of clinical trials
- ⇒ Improving hospital recognition as clinical research centres of reference
- ⇒ Engaging in a highly dynamic clinical research environment to improve the overall quality of care and knowledge transfer

Principal hurdles identified are interoperability, legal (data protection) and ethical issues, and the integrity and trustworthiness of data. Therefore, user groups were integrated into the development process at a very early stage (De Moor *et al.*, 2014). The EHR4CR project was pointing to conditions within which the risks and disadvantages of cloud can be mitigated and the opportunities and benefits realised.

Based on findings from the eHealth cloud projects reviewed in Section 2.2, the research will further discuss the major challenges identified in Section 2.3.

### **2.3 Challenges Limiting eHealth Cloud Adoption**

As seen from the reviewed projects, technology plays an important role in healthcare, with cloud computing slowly beginning to make its mark. However, despite the important benefits of cloud computing, there are several other

significant challenges and barriers to implementation that are responsible for its slow adoption (Gupta, 2015; Parker, 2018).

Healthcare lags compared to most other industries in the adoption of cloud technology. Most healthcare organisations are subject to workflows comprised of paper-based healthcare archives, duplication of tests, film-based radiological images, handwritten summaries, disjointed IT systems, and silos of information. Information sharing across these healthcare providers is disorganised, and data portability is uncommon. Most healthcare providers depend on obsolete technology for their information-sharing needs, and collaboration and coordination of care processes are major challenges. Other major challenges (Gupta, 2015) limiting the adoption of eHealth cloud are:

- ⇒ The digital gap: Some of the best healthcare organisations, in relation to adoption of cloud technology and delivery of great quality healthcare services, exist in major towns and cities. However, the situation is often different in rustic towns, where healthcare organisations can lack even basic infrastructure, not just advanced technological infrastructure. This highlights the fact that practitioners working in rural towns may have limited knowledge about technology in comparison with their colleagues in major towns.
- ⇒ High costs of adoption and implementation of various dissimilar infrastructural mechanisms: The widely accepted fact is that traditional technology entails the use of many infrastructures and workforces to implement. It is therefore necessary to have a shared and integrated network infrastructure, which can form the 'foundation for connected

health'. To get the most out of technology investments, healthcare organisations require an integrated information technology (IT) network that supports various units to team up and communicate effectively. The cloud can perform as this foundation for connected health to support a variety of complex, dissimilar, and mission-critical applications.

⇒ Apprehensions about patients' data confidentiality and security issues:

This is slowing down the acceptance of cloud technology. As patients' data is located outside the healthcare organisation's facility, there is apprehension about the increased risk of sensitive data being lost or misused or getting into the wrong hands.

⇒ Obtaining the trust of all the stakeholders: This is also a massive

challenge, yet gaining the trust of both internal and external stakeholders is very critical to the adoption of cloud technology. Some healthcare providers still do not appreciate the significance of the cloud as an enabler of faster, safer, efficient, and more effective healthcare. Thus, providers may be reluctant to make investments in cloud technology.

⇒ Cultural concerns and change management: Implementing cloud

technology encompasses major modifications in the workflow of the healthcare providers. Healthcare organisations have been reliant on legacy systems and workflows, many of which are obsolete and not efficient. However, many healthcare organisations circumvent updating their IT infrastructure because of lack of funds and a trend to avoid capital expenditure on new technology. Moreover, healthcare stakeholders have conventionally been resilient to change.

## **2.4 Conclusion**

Many challenges have been identified and discussed through the review of literature and specific projects. However, there is no indication of the relative significance of these challenges. As such, it is important for the next chapter to investigate this.

## **Chapter Three**

### **3 Assessing Challenges in Adoption of eHealth Cloud**

The purpose of this chapter is to understand the significance of factors influencing the adoption of cloud computing in healthcare. For the purposes of this research, in-depth (telephone-based and unstructured) interviews were used to identify participants' feelings and opinions regarding this particular research subject.

The main advantage of telephone-based interview is that they involve contact between researchers and participants and also eliminate nonresponse rates, but researchers must develop the necessary skills to successfully conduct an interview (Langkos, 2014). In addition, general, open-ended questions are asked to allow participant to create opinions before responding, offering flexibility in terms of the interactions during the interview and thereby facilitating the generation of conclusions regarding the research subject. However, there is increased risk that the interview may deviate from the specified research aims and objectives. Therefore, the data collection tools involved the use of a semi-structured questionnaire which was used as an interview guide for the researcher and a Dictaphone to record the interviews, when permitted. Certain questions were prepared for the researcher to guide the interview towards the research objectives, but additional questions were asked during the course of the interviews (a detailed interview guide and summary are presented in Appendix E and Appendix F - Interview Question Guide).

During the expert interviews, study participants' responses were informed by their perceptions and experiences, and the methodology for this study guided the

interviews. This chapter focusses on presenting and discussing the findings from the interviews and comparing them to relevant academic literature (Whitten and Kuwahara, 2004; Bath, 2008; Robert *et al.*, 2009; Ward and Sipior, 2010; AbuKhoua, Mohamed and Al-Jaroodi, 2012; Zanaboni and Wootton, 2012; Lian, Yen and Wang, 2014).

### **3.1 Data Collection Process/Methodology**

A trial interview was conducted for two participants (not part of the four main participants) to test the cogency of the research questions and feasible responses from intended participants. This data collection phase was initiated with the conduct of four in-depth interviews during the timeline in Table 3.1 for a better understanding of the subject matter.

Invitation e-mails containing the research proposal, institutional approval, and written consent were sent from August 2016 to the selected participants to get their acceptance of participation in the research. More specifically, the researcher asked them to participate in the research after explaining the nature and the scope of the study. In general, the respondents were willing to participate, and the interviews were conducted between September and December 2016. The interviews took place over telephone and Skype calls and lasted approximately thirty to forty-five minutes. Some interviews were recorded if permitted; otherwise, notes were taken to help the researcher analyse the gathered data. It should be noted that the conversations were pleasant and flowed smoothly.

The results of this interview phase are illustrated in section 3.3.2. Open coding was used for the in-depth interviews with the help of qualitative analysis software



NVivo. Focussed coding was also used with the help of NVivo, which used the initial codes as a basis. Memos were written during the entire process of collecting and analysing data as this facilitated reflection on the collected data. In addition, careful comparisons between respondents' statements and codes were made without being restricted to interpreting participants' words within a framework of properties and dimensions.

As a framework, this research focusses on a specific challenge with relatively high intensity to further understand its impact on the adoption of cloud and the underlying reasons through (validation) interviews and support from literature.

Timeline	Data Collection	Data Analysis	Analysis Method
August 2016	Conducted pilot study interview		
September to December 2016	Conducted and transcribed four in-depth interviews	Initial codes Focussed codes	Open coding with NVivo software Memo writing Focussed coding with NVivo software

**Table 3.1 Data Collection Process**

### **3.2 Background of Study Participants**

The study participants were identified through a web search of the appropriate people with roles in healthcare record-sharing projects, health IT departments, and research contribution in health informatics and the field as a whole. An e-mail consisting of the letter of introduction and purpose of the interview were sent to the fifty selected participants; however, only nine people responded, out of which six agreed to be interviewed and three responded to decline an interview as they were not available. One of the six participants subsequently withdrew on the basis

that his/her experience did not include cloud eHealth and he/she felt that he/she could not provide informed views on the interview questions. In addition, one interview response was not included in this analysis because of the time interval of the project. The remaining interview responses form the basis of these findings.

The participants of the study included an IT manager and specialist with over thirty years' experience in the installation of clinical systems in large healthcare organisations and maintenance of health information systems. Another participant was a researcher involved in a healthcare data-sharing project and who worked in an organisation that provided healthcare data-sharing solutions to healthcare organisations. The next participant was a professor in a radiological sciences department and a top researcher at a healthcare imaging informatics group. The last participant had several years of experience in healthcare information sharing and led a national healthcare record-sharing project. These participants were based in the United States, Australia, Ireland, and Portugal.

### **3.3 Scope of Study**

Two themes are the guiding factors for this research, one of which focusses on adoption of cloud computing and its application across international borders. Based on the complexities involved with international laws on healthcare and a lack of relevant contacts in the subject area abroad, this theme is considered to be out of the scope of this research.

Hence, this study's main focus is the effectiveness of current healthcare security practises/culture, which involves maturity levels of cloud computing adoption in

hospitals, deeper understanding of current practises, and challenges in the research area.

This study researches the aspects that influence cloud computing adoption in healthcare and their importance and intensity. Careful questioning was used to obtain responses that reflect specific challenges, how intense these are perceived to be, proposed processes/technology solutions deemed fit for the challenge, intensity of organisational culture versus technical solutions available in eHealth cloud.

The results identify the challenges and their intensities, proffered solutions/processes from professional viewpoints for the adoption of cloud computing in healthcare. Obtaining insights into these challenges from the experts' perspectives gives the study stronger reliability and novelty.

### **3.3.1 Study Question**

The main interview question, which is the focus of this study, is the following:

⇒ Technical security or organisational culture: Which is the major reason for the limited adoption of eHealth cloud?

Whilst the technical and organisational culture themes are distinct, there are significant connections between them. Furthermore, participants' responses to interview questions often addressed more than one theme. In those cases, the interview data are described where they appear to fit most logically.

### **3.3.2 Findings on the Factors Limiting Adoption of eHealth Cloud**

These findings were obtained from the interview participants' statements, which are referred to with the use of direct quotes. To support the opinions of these experts in the field, relevant literature were referenced.

#### **3.3.2.1 Technical Challenges**

##### **3.3.2.1.1 Service Reliability and Availability**

'There are several factors that affect the adoption of eHealth Cloud. Technical security is one of the first reasons people cite, but it is not the most important. Whilst technical security is a concern, it is not a barrier. Most of the cloud providers are regarded as technical cloud architects (TA1), providing all the required technical security and access control mechanisms attached to their data centres. Hence, the technical security limitations involve integrity and access control problems but also include maintaining a resilient backup in case of disaster recovery, data/service reliability, systems interoperability, database security, transmission speed performance, and configuration flexibility' stated Participant 1. Other technical challenges include the use of earlier/older healthcare applications which are not cloud-computing compatible.

Next is the need to assure the hospital management executives about the uninterrupted availability of data when it is transferred to the cloud. Participant 2 mentioned that 'Medical practitioners require high availability of the cloud services, and service and data availability is crucial for practitioners who cannot effectively operate unless their applications and patients' data are available. They

are expected to be available and reliable without interruptions or performance degradation’.

Operationally, the reality is that cloud services could experience failures due to software and hardware faults, network faults, security attacks, and natural disasters, among many other occurrences. However, medical applications are critical and must guarantee very high performance, availability, and reliability standards. For this reason, clouds must provide availability and mobility support to medical data storage and make processing services accessible through the Internet. Although hardware and software installations, upgrades, and reconfigurations could be managed without any service interruptions for the hospital (Sasse, Brostoff and Weirich, 2001), increased complications still exist when managing, securing, and maintaining these dynamic environments based on the total dependence on Service-Oriented Architecture (SOA) web services, Cloud-based Service Providers (CSPs) and Software-as-a-Service (SaaS) solutions (Ammenwerth *et al.*, 2003).

Regardless of some widely advertised CSP disruptions, cloud-based services have been extraordinarily consistent, which may be nurturing complacency amongst hospitals that are very dependent on them. The data compiled by AppNeta on the uptime reliability of forty of the largest providers of cloud-based services offers some indicators on the performances of CSPs. The total industry yearly average of uptime achieved for all the CSPs observed is 99.948 per cent, or 273 minutes of unavailability per year. The best providers accomplish 99.9994 per cent, or three minutes of unavailability each year, whilst the worst providers

achieve 99.92 per cent, or 420 minutes of unavailability each year. These indicators reveal low outage risk from cloud providers (Thibodeaux, 2011).

#### **3.3.2.1.2 Web Performance and Latency**

In addition to the challenge of data availability, there is also the challenge of slow performance due to low bandwidth, resulting in latency. Remote rendering does not always provide sufficient display latency for all medical applications when the server must be accessed over the Internet; neither does high bandwidth network in a remote data centre overcome the limitations of relatively low bandwidth and shared communication links. Such delays in accessing healthcare records stored in the cloud may cause dangers to a patient's life, especially during surgery.

'There is the need for fast performance of web solutions and reduced waiting time for healthcare records to load. Presently, there are too many vendors and solutions which create questions related to availability such as: How do the solutions deliver data? Is it in a very quick manner? Is it implemented at an urban or remote area? How are delayed data transmissions (latency) over the network overcome? Where is the data stored?' mentioned Participant 3.

#### **3.3.2.1.3 Disaster Recovery**

This is a part of service reliability that emphasises processes and technology for continuation of applications, data, hardware, communications, and other IT services in the event of a disaster. The process of creating a disaster recovery plan begins with identifying and ranking applications, services, and data and defining for each the acceptable downtime before there is a significant life-threatening impact. 'Presently, cloud Service Level Agreements (SLAs) provide

inadequate guarantees in case of a service outage due to a disaster, and the healthcare industry's requirement of availability and consistency of information can be a matter of life and death' stated Participant 4. This is further supported by Cloud Standards Customer Council (2015), according to which the disaster recovery provisions of 99%+ SLAs in cloud computing (approximately 4 days of downtime a year), may not be adequate for specific applications and business needs (Cloud Standards Customer Council, 2015).

The recent closure of Google Health, a cloud application service aimed at providing free access to people to store their personal health and wellness information, further brings an insight into the risk of adopting public cloud services for sensitive data processing. Many people wondered how users of this service would either recover their data or be sure that it has been erased when the service went offline. It is worth mentioning that uncertainties and lack of transparency are present in the cloud framework, such as abrupt failure of services (Huang *et al.*, 2005).

Furthermore, 'counter to the generalisation that a centralised national database for healthcare data is less secure and faces more security risks than regional-based databases, it has been shown from experience that the security risk is actually less when using a centralised database for healthcare data than when using a regional database. This is because the centralised database is usually the Technical Cloud Architect (TA1) type of data centre with full resilient backup for disaster recovery, and the access to the data centre is incredibly well controlled and also considered more cost effective' contributed Participant 3.

#### **3.3.2.1.4 Integration and Interoperability**

‘A crucial element to healthcare beyond the IT field is the consistent transmission of commonly understood information to enable corresponding patient care’ stated Participant 3. Different medical practitioners have different terminologies and requirements. To provide an end-to-end system that fully integrates all patient information (emergency and in-patient care, pharmacies) entails standardisation and interoperability.

Interoperability involves defining an agreed-upon framework or open protocols that allow easy servers and data integration amongst different cloud service providers or cloud types, including secure information exchange and services’ integration (Dünnebeil et al., 2012). An approach is to use Service-Oriented Architecture (SOA), which provides interoperability between the cloud components and users by making services easily accessible through standardised models and protocols without underlying infrastructures, development models, or implementation details (AbuKhoussa, Mohamed, and Al-Jaroodi, 2012). Another approach is to establish a ‘common language’ between the systems. As well as having common message formats, the information carried in messages will often contain identifiers to allow recipient systems to transform and process content intelligently. These common identifiers include common coding schemes, classifications, and vocabularies for fields, which are stored somewhere accessible by both sides (eHealth Network, 2015; NHS England, HSCIC, South, 2015).

Similarly, there is the challenge of integration; there are several strong security solutions, but they are not totally integrated. The development of information



systems within separate departments or hospitals resulted in incompatibility amongst them and created problems in exchanging or transferring data. To resolve this, the use of established electronic record architectures in the design of new systems is recommended. Related to this is the lack of standards for healthcare data, further complicating the difficulties of transferring and sharing data across systems (Anderson et al., 2007; Sharma et al., 2009).

Certain standards are needed to help facilitate the exchange and storage of data within the cloud through mutual and merging components. Hospitals have several standards development organisations (SDOs) to develop qualifications and standards to support healthcare informatics, information exchange, and systems integration. These standards are created for specific domains such as pharmacy, medical devices, imaging, and insurance (claims processing) transactions (Thilakanathan, 2016).

‘There are also many healthcare standards, including digital imaging and communications in medicine (DICOM), health level seven (HL7), and international classification of diseases (ICD). However, there are also differences with the implementation of these standards’ mentioned Participant 2. For instance, many manufacturers implement DICOM standards differently, so data exchange and system interoperability remain challenging. Other challenges include incompatibilities with the hospitals’ visions, operational processes, lack of transparency of off-loaded data, and applications.

Finally, the eHealth cloud must be integrated within the clinical workflows (business processes, and operations and maintenance (O&M)). In order to encourage the acceptance of the eHealth cloud (Moreno-Conde *et al.*, 2015).

#### **3.3.2.1.5 Data Portability**

‘Another challenge that influences hospitals’ readiness to adopt cloud computing is the concern about the ability to switch to another cloud vendor or back to the hospital database without disrupting operations or introducing conflicting claims to the data’ stated by Participant 1. Whilst there are rules and standards to provide interoperability amongst cloud providers, they are still inadequate to guarantee data, applications, and services portability.

Data structures and services interfaces differ from one cloud provider to another. This can make the migration of data, applications, and services from one cloud provider to another or back to its local IT environment difficult. Facilitating migration is expensive, especially if there is a large amount of data stored in the cloud, as in healthcare. This results in a dependency on a particular CSP for service if data portability is not allowed (Thilakanathan, 2016).

This risk reveals the need for Service Level Agreement (SLA) that discusses termination rights, rights to access and retrieve data at any time, termination assistance in moving to another provider, and ‘cure periods’ to allow breach of contract to be resolved before the provider terminates or suspends services.

#### **3.3.2.1.6 Data Quality**

In addition, quality is an issue that can affect successful development and implementation. The quality, both actual and perceived, of data entered into systems and then utilised for healthcare is critical not only for ensuring systems are utilised but, more importantly, for the safety and well-being of patients. All important decisions regarding a single individual or society’s health are taken

depending on the data provided. Hence, the patients' data stored in the cloud must be consistent and constantly in a valid state regardless of any software, hardware, or network failures.

The imperative for patients' data that are complete and correct will increase as lifelong electronic healthcare records are developed (Berner and Moss, 2005), for care records developed prospectively as individuals are born, and also for those developed retrospectively using data accumulated over an existing person's lifetime to date. Whilst the cloud services must be error-free, they must also be easily configurable to meet different needs with minimum effort and cost (Youssef, 2008).

Furthermore, 'it is important to ensure the cloud provider cannot access or use the hospitals' database/data' mentioned by Participant 4. This relates to the need for efficient security mechanisms with a wide range of security requirements amongst healthcare providers. A hospital's security requirements and policies must be fully reflected in cloud services. This service should not lead to high computation or communication costs, rendering the cloud economically inaccessible (Yang et al., 2010). In addition, the cloud should be flexible in adding new needed services to support healthcare processes and requirements whilst being easily configurable to meet different needs with minimum effort and cost (Vaquero et al., 2009).

#### **3.3.2.1.7 Access Control Solutions for Clinical Workflow**

A variety of technical issues create barriers to more widespread adoption of eHealth cloud. Implementing the paradigm in a clinical setting is more complex

than connecting a computer to the Internet or installing software on a system. The paradigm must conform to the workflow of the hospital, or the workflow must be modified so that the paradigm does not hinder it (Hersh, 2004). To achieve these conditions, 'healthcare administrators are challenged to reach an optimum level of security whilst negotiating the trade-offs associated with the expense, acceptance, and usability of potential solutions which must respond to the unique requirements of the hospital' stated by Participant 1.

User authentication mechanisms for data access controls and audit are vital to any comprehensive security solution. This is the process of identifying and confirming the identity that a user is affirming to be and then granting access privileges to resources based on that identity. There is a range of possible technical solutions for authentication; these solutions vary in terms of their cost, complexity, and assurance levels. The challenge of identifying an optimum solution lies in the fact that there are a multitude of forces acting on the design decisions and ultimately the adoption of authentication mechanisms (Heckle and Lutters, 2011).

In addition, addressing workflow in data access security is a difficult problem with many socio-technical complications. Whilst there has been advancement in the development of data access technologies, when the technologies are placed in context, they rarely work as intended or are difficult to integrate into the system (Orlikowski, 1992). In a healthcare environment, there is a need to balance information security without impeding the quality, timeliness, and effectiveness of healthcare delivery (Adhikari and Lapinsky, 2003; Bardram and E., 2005).

With any authentication mechanism, there is an inherent trade-off between security strength and usability (Adams and Sasse, 1999). Mechanisms that are easy to use frequently relinquish some security strength, just as those mechanisms that offer stronger security often prove more cumbersome to use. Mechanisms that provide usability and strength come with greater financial costs. Whilst there are many security approaches available, the current authentication method of choice for most industries is the traditional username/password pair. This method of authentication has the advantage of being both simple and economical.

However, 'problems arise when medical practitioners must manage a large number of unique username/password combinations as they navigate all of the applications required for the job' by Participant 1. Studies have shown that the problems with username/password authentication are related to human cognitive limitations at the core of the issue (Adams and Sasse, 1999; Sasse, Brostoff and Weirich, 2001; Weinshall and Kirkpatrick, 2004). There is an increasing push towards stronger, more abstract passwords. However, these are difficult to remember, causing users to be reluctant to change them, or they write them down, thus subverting the mechanism and causing a security breach.

Currently, single sign-on (SSO) technologies have emerged as an effective means of addressing these authentication challenges. SSO provides practitioners the ability to log in to the network once and then be able to navigate the countless number of applications seamlessly without the need to enter authentication credentials for each application. SSO promises to improve usability of authentication for users of multiple systems, increase compliance, and

help curb system maintenance costs. However, difficulties emerge in trying to fit authentication that is individually oriented into a hospital that is collaborative in nature.

To summarise, SSO authentication approaches improve security by increasing user compliance through more usable software; for collaborative technologies to be effective, technology must be flexible and adjust to the situation. However, 'improving the overall usability of authentication solutions and the effectiveness of the technology itself is not enough; the context within which the technology is used will greatly affect its usefulness. This is considered one of the reasons for the limited adoption of the technology as it is not engineered to fit within the healthcare context' by Participant 4.

Lastly, these limitations have revealed that there are weightier security challenges limiting the adoption of the cloud computing paradigm than only access control and integrity. These challenges are beyond security requirements only but exist also in terms of functions, operations, users, auditing, management, and quality of service requirements.

#### **3.3.2.2 Organisational Challenges**

The challenges between organisational structure and technology have been in effect for a long time. It is now well established that when technology is implemented, organisational effects will be seen. Thus, organisational and social issues are critical in the implementation of information systems (Monrad, 2007). Organisational challenges are mostly responsible for the most significant obstacles for eHealth cloud (Magrabi et al. 2015). Therefore, identifying eHealth's

organisational problems and designing solutions for these problems can be of help for the future of eHealth development.

The low utilisation of eHealth cloud is a serious problem which is often underestimated in terms of organisational issues. Increased adoption of eHealth cloud requires answers to these issues of organisational culture resistance, trust, and costs, amongst other aspects.

#### **3.3.2.2.1 Financial Costs**

The rising cost of healthcare throughout Europe has put e-Health high on the political agenda; the 'Europe 2020 vision' is opening the way for eHealth services as these are believed to prospectively reduce public expenditure on healthcare (Glazer and Ruiz-Wibbelsmann, 2011; Ranschaert and Binkhuysen, 2013). However, the costs of eHealth cloud do not only relate to the initial spending required to have an operational implementation but also to the maintenance and management costs required to ensure the cloud works as expected. Furthermore, 'the first hospitals which chose to implement cloud may enjoy little or no benefits since they will need to wait for other hospitals to implement a similar solution before communication of medical data can be experienced' Participant 2. In other words, healthcare organisations must calculate the cost and benefits of an eHealth cloud before determining the feasibility of adoption (Hill and Powell, 2009).

'Healthcare management executives are constantly looking for cost reduction, so IT professionals must balance associated risks with cost involved' by Participant 1. Another major factor in adoption is economics; 'many financial factors drive

decisions in healthcare management, for instance, funding from country, state, county, or government/nongovernment agencies for the overhead cost of implementing the system. This also applies to international efforts, so several factors apart from security majorly determine the decision of a hospital's adoption of cloud. Mainly, healthcare executives are looking for ways to cut costs yet improve clinical care' by Participant 1.

Similarly, financial investment is required to develop, implement, and maintain eHealth, and lack of financial support and high initial costs were identified as barriers to adopting cloud computing in healthcare (Bath, 2008). Inasmuch as hospitals are built to provide healthcare services, they are also commercial organisations. In most cases when cloud telemedicine is adopted, stakeholders bear the overhead costs, whilst the patients get the benefits. Aspects that require attention include how to manage shared resources, production capacity, marginal costs, and the use of salaries and charges as proxies for opportunity costs. Also, organisational executives may be unconvinced about such expansions, particularly when they are satisfied with current methods of working, wish to maintain the status quo, and perceive such a change as diverting financial resources away from under-resourced clinical care. The diversion of funds allocated for local developments was cited as another major reason for the limited progress in implementing the cloud strategy (Burns, 1998).

In addition, healthcare providers require good performance of the cloud services. Service performance is critical to healthcare providers; they cannot operate effectively unless their applications and patients' data are readily available when required. However, having high performance services can be costly. A trade-off



between acceptable performance level and service cost is, therefore, required (Lian et al., 2014). Beyond the general belief that trust in data security and privacy by users is at the heart of the resistance that healthcare managers have towards the cloud (Li et al., 2011), economics and cost have been discovered to be central to this resistance.

Despite that, one advantage achieved from the adoption of cloud computing technology is to reduce operating costs and increase the relative operational benefits for a given hospital (Premkumar et al., 1999). However, the adoption of cloud computing technology is usually a large project and a huge undertaking for hospitals. The given hospital or group of hospitals must have a sufficient budget, adequate human resource support, ample time, and executive managers' involvement for the adoption of cloud computing technology to be received in a positive manner. To that end, these resources are highly critical to the success of adoption.

#### **3.3.2.2.2 Organisational Culture Changes**

The adoption of eHealth cloud will necessitate major changes to clinical and business processes and to the organisational boundaries in the healthcare industry. This challenge is based on the changes that eHealth cloud will present to participants. 'Hospitals have ingrained culture, policies, procedures, workflows, medical processes, and documentation; however, transferring to cloud technology may change the traditional ways of sharing data and affect employees' informed by Participant 3, resulting in resistance, which is a common management challenge in adopting cloud computing. It is necessary for a plan to

implement a smooth transition to the new technology (AbuKhousa, Mohamed and Al-Jaroodi, 2012).

Overall, the healthcare executives and workers are not barriers, but they must be educated on this topic and completely understand the requirements and challenges in adopting the paradigm.

#### **3.3.2.2.3 End Users' Assessment and Trust**

Medical practitioners and patients are the end users of an eHealth cloud. 'A key challenge for its adoption is, therefore, gaining the end user's trust in cloud technology. Various broadcasts on the insufficiency of eHealth have arisen in UK news in recent years' stated Participant 2. A leading example of this was in 2009, when the National Health Service (NHS) in England lost thousands of medical records (Savage, 2009) due to a lack of security in their computer systems. More recently, in July 2011, the NHS was once again in the spotlight when computer criminals attempted to gain access to their systems that held patient medical records (Lo *et al.*, 2013). Most recently, in May 2017, the NHS was crippled by the biggest ransomware (WannaCry) outbreak in history (Graham, 2017).

From the frequency of these alarming reports on the issues related to e-Health, one can understand why patients may feel uneasy about medical facilities storing personal data in an eHealth environment. The lack of trust in eHealth is also a key issue with medical practitioners. Rather than concerns over security, there are two primary reasons for this: resistance to change and lack of education and training on the usage of the technology (Vinegar, 2013).

Compared with the patients and executive organisational staff, practitioners may accept technology decisions differently. Predominantly, practitioners are not technology literate in spite of their general competence and learning capacity. Having experienced highly demanding educational and specialised training, many are experts in their own profession and accustomed to practising in a particular way or style similar to that in which they were trained. From prior studies, practitioners are usually unenthusiastic about the implementation of information systems that interfere with their traditional routines; therefore, they seldom give positive responses about the new system (Anderson, 1997; Anderson and Aydin, 1997).

In addition, practitioners usually practise with relatively high autonomy. Thus, individual and collective outlooks towards the perceived value of IT systems may lead to a more general resistance to using these systems. Such resistance from practitioners and executive organisational staff can create further problems after systems are implemented, and the limited use of health informatics applications has meant that their potential has not always been realised. This emphasises the need not only to involve practitioners in the development of systems and the interpretation of results but to also provide sufficient explanations and information for practitioners to trust the systems (Berner and Moss, 2005). Without support from medical practitioners, adoption and use of eHealth will greatly lag; hence, their trust in the system is essential. With regards to the patients' perspective, assessment of their approval on the overall healthcare provided by an eHealth cloud is equally important. Traditionally, patient approval is the measurement of the patient's opinion of the quality of service provided during treatment within a

healthcare environment (Gill and White, 2009). Ensuring positive patient satisfaction of eHealth cloud not only proves the feasibility of its implementation but may also ensure that wider adoption of eHealth cloud takes place.

### **3.3.2.3 Legal Challenges**

The use of cloud computing in healthcare results in many legal issues such as contract law, intellectual property rights, data jurisdiction, and privacy (Kuner, 2010; Ward and Sipior, 2010; Pearson, 2009). Amongst them, 'data jurisdiction is a major concern' stated Participant 1. Physical storages for the cloud are typically widely distributed across multiple jurisdictions, each of which may have different laws regarding data security, privacy, usage, and intellectual property (Kuner, 2010; Ward and Sipior, 2010). For instance, privacy acts such as Health Insurance Portability and Accountability Act (HIPAA) and Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) can be applied to data only within the United States, whilst the Personal Information Protection and Electronic Documents Act (PIPEDA) operates within Canada. The cloud provider could (without notice to the hospital) move part of the hospital's information to another jurisdiction, resulting in patients' data having more than one legal location at the same time, with contradictory legal consequences (Health information privacy, 2015; Justice Laws - Privacy Act, 2016; USA PATRIOT Act, 2001).

There is also a requirement for additional harmonisation of legislation regarding the processing of health data in cross-border healthcare services, and a European directive is obligatory to guarantee the safety of patients. For example, the European Society of Radiology has many publications in which they have expressed their concerns about teleradiology and have also provided guidelines

and recommendations for the development and use of teleradiology services within the EU (ESR, 2012).

### **3.3.2.3.1 Standards**

There are still no clear or adequate guidelines for clinical, technical, and business practises of healthcare in the e-context. This includes the lack of standards for medical informatics, policies, interoperability, and transmission methods in eHealth cloud. Hence, the participants in eHealth cloud do not have a foundation to start offering and using it. Thus, more issues and problems may occur due to this shortage, and as a result, technical, social, and ethical concerns will arise (Lo *et al.*, 2013).

Generally, 'there are some standards and classifications for health information systems, some of which can be adopted for the eHealth cloud' informed by Participant 3. An example is the International Classification of Diseases' tenth revision (ICD-10) issued by the World Health Organization (WHO), (*International Statistical Classification of Diseases and Related Health Problems ICD-10*, 2010; NHS, 2011b), which defines a medical classification list for the coding of diseases, signs or abnormal findings, complaints, social conditions, and external causes of injury or diseases. Another classification is the Systematized Nomenclature of Medicine (SNOMED), which was designed as a detailed categorisation of clinical medicine for the purpose of storing and/or retrieving records of clinical care in human and veterinary medicine (NHS, 2011b). The eHealth cloud developers can agree on adopting some of these defined standards and classifications to enable interoperability amongst different organisations.

However, even if the eHealth cloud adopted some of these defined standards and classifications for improved data sharing amongst several healthcare organisations, legal issues such as liability and concerns related to patient privacy and safety would yet remain unsolved (Pohjonen, 2010). This legal insecurity is certainly one of the main reasons for the rather slow implementation of eHealth cloud in Europe. For instance, it should be clear for patients if the physician providing the services is properly licenced and accredited and in which country the liability of the physician is to be addressed: the country where the patient is examined or the country that is the residence of the physician.

#### **3.3.2.3.2 Data Privacy Legislation**

The governments of various countries in the mature markets are currently faced with resolving and managing the collective needs for privacy and freedom of information. On 1 July 2012, the Article 29 Data Protection Working Party (the independent European advisory body on data protection and privacy) adopted an opinion on cloud computing (WP196) that is expected to be used as a standard guide for cloud requirements in the EU (*ARTICLE 29 DATA PROTECTION WORKING PARTY*, 2012). It stated that the cloud client should be considered as the 'data controller', whilst the CSP acts as the 'data processor', except where the CSP processes the personal data for its own purposes. An effect of this statement is that the applicable law will usually be the legislation of the country in which the cloud client is established rather than the place where the CSPs are located.

Although the European Commission's standard contractual clauses offer satisfactory safeguards, they do not apply to a situation where the CSP acting as

a processor is established in the EU and uses non-EU subcontractors. Because the location of data is abstracted in cloud computing, a CSP could move data between countries and jurisdictions without the awareness of the data owner. In fact, data could reside in more than one country, each having a different legal stance on privacy. As a result, the European Commission is working on a prohibition of corresponding disclosures of personal data to be included in the future General Data Protection Regulation, subject to specific exceptions.

The following section will discuss the influence of these findings on the research.

### **3.4 Influence of the Identified Challenges Limiting eHealth Cloud Adoption**

At the onset of this study, the researcher had the hypothesis that technical challenges were the major factors inhibiting the rate of adoption of cloud computing in healthcare, particularly in Europe. However, after the preliminary interview, it was realised that technology does not have as much impact as a factor in inhibiting the adoption as organisational challenges do.

Based on this research and interviews, the findings were confirmed to be realistic in the subject area and were later supported by a literature review. This reveals that there is a need for in-depth research in this subject matter. Furthermore, available security solutions for utilising eHealth cloud technology would not solve the challenges presented in this chapter, but assessing their organisational implementation could reassure end users that the eHealth cloud will continue to follow an inspirational model of good working practises for years to come.

With the increasing pressures of citizens' healthcare management and current financial crises such as rising costs of services and innovations leading to more

funds required for healthcare trusts, especially in the UK, this research is considered valuable in helping to avoid huge financial debts. It also provides information and knowledge to the healthcare chairs and staff who are currently considering the adoption and implementation of eHealth cloud computing to maintain a high standard of healthcare services for citizens (Horsley, 2015).

### **3.5 Chapter Conclusion**

To implement eHealth cloud, the financial costs to be allocated depend on what the challenges are, their criticalities, and their impact. However, most costs will be allocated to organisational challenges regarding security, which includes workflow and implementation.

Hospital executives are the primary decision makers regarding cloud adoption, and project managers must satisfy their requirements when implementing an eHealth cloud (Whitten and Mackert, 2005). Hence, it can be inferred from the interview findings that the organisational challenges regarding implementation of technical security solutions are amongst the major limiting factors for the adoption of eHealth cloud. As such, the next chapter focusses on developing a theoretical framework for the proposed novel security maturity model to help healthcare organizations assess and improve their security practices and processes in the eHealth cloud.



## **Chapter Four**

### **4 Theoretical Framework for Proposed Maturity Model**

With the aforementioned challenges in healthcare, the need to adopt and implement cloud computing in this field as a whole is becoming more apparent.

This research proposes solutions to assess the identified challenges with high impact with a view of capitalising upon the benefits presented by cloud computing, its universal connectivity, scalability, and flexibility. These promising features offer a new opportunity of achieving affordable healthcare services and reducing personnel strain in hospitals.

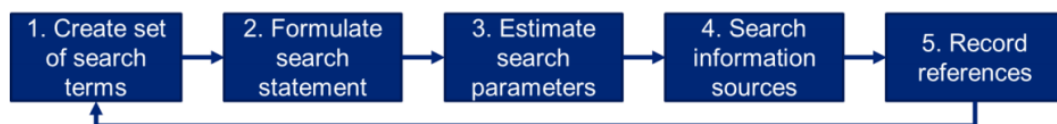
#### **4.1 Systematic Literature Review**

To gain awareness of the existing research about this subject, a systematic literature review (SLR) was performed. In this SLR, two compounded search terms, 'cloud security maturity model and electronic healthcare', were used at two electronic information sources specific to healthcare and computer science/cyber security. This resulted in a set of important sub processes and quality factors and a clarification of the research gap. The choice of the two search terms was based on a literal analysis of the research title and the intention was to identify resources from both electronic healthcare and cyber security domains.

##### **4.1.1 Systematic Literature Search Approach**

The research methodology ensured logical and systematic reviews based on concept-centric frameworks. The latter were employed since they allow detailed explanation of the process, are comprehensive in scope, and provide an

opportunity for reproducibility (Webster and Watson, 2002; Okoli and Schabram, 2010). The research parameters and search terms were formulated according to a predefined set of rules of SLR, which informed the combination of search terms. To expand on the identification phase, the SLR with five main stages (Duff, 1996) was adopted because its processes follow a clear and repeatable protocol (Figure 4.1).



**Figure 4.1 Systematic Literature Search** (Duff, 1996)

During the first stage, a broad set of search terms was developed to guarantee a result of domain-related literature. To achieve this, a conceptual taxonomy was adopted that arranged search terms in a framework of their synonyms, broader, and narrower terms (Duff, 1996).

Secondly, the search statement was formulated. The identified maturity models are included if they define steps towards improvement in maturity of capabilities. In addition, the domains in which the maturity models are used should be cyber security, IT in healthcare, or a combination of before mentioned. The best search strategies adopted were the proper use of Boolean operators, which combined both natural language and phrasebook (Duff, 1996). For this research, the search statement formulated included

(‘Cloud security maturity model’ or ‘cyber security maturity model’ and ‘electronic healthcare’ or ‘capability maturity model in electronic healthcare’).

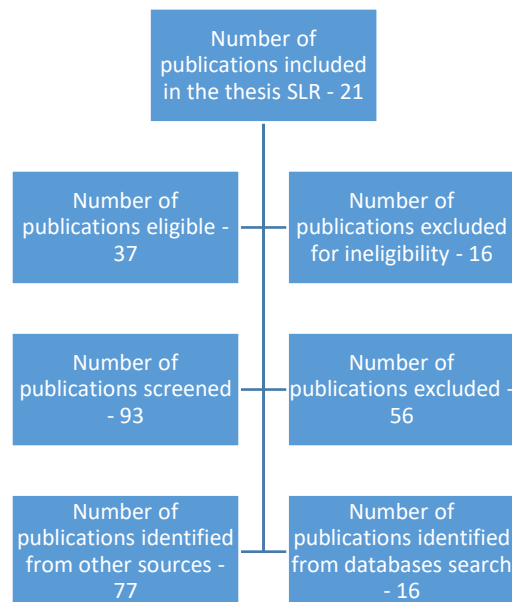
In the next stage, the search parameters were established. Four major parameters were used in this research: formats of literature such as books, journals, conference publications (formal); subject domains of research conducted (disciplinary); the year when the research was conducted (temporal); and the geographical area in which research was conducted (spatial) (Duff, 1996). Presently, there is relatively limited literature available in the field of cloud security maturity assessment in healthcare; therefore, to ensure all the maturity models compared are rooted in well-structured concept, exclusion criteria is developed. The identified maturity models are excluded if the maturity models have no information regarding the models and theory they are based upon. The established disciplinary parameter excluded research with a primary subject domain that was not cybersecurity. There were defined cybersecurity maturity models. However, this research did not include studies conducted in developing countries to define spatial parameters. Lastly, cybersecurity is a fast-evolving field, so a temporal constraint was defined to include only relevant literature, starting in 2010.

The search for information sources was the fourth stage. The main information resources were obtained online. To keep the research rigorous, three proxies of search engines were included, all with a different focus. For this research, the information sources specified for the healthcare were Springer and PubMed. The information sources for computer science and cybersecurity literature were the Association for Computing Machinery (ACM), Elsevier Science Direct, IEEE Computer Society Digital Library (CSDL), and the Association for Information Systems electronic library (AISel). Lastly, Google Scholar was included with a

general focus, and this generally contains the most articles and may in some cases include publications of the other chosen databases; however, these could not be accessed through the proxy used for Google Scholar and are thus identified separately.

Finally, the references of these publications were recorded and included in the bibliography. In Figure 4.2, the overview of the search and exclusion process is provided. The process consists of identification, screening, eligibility, and the analysis of included publications. (The identification process was previously discussed.) The screening included the titles, abstracts, and meta-data. Based on the screening of the title and abstract, out-of-scope literature was excluded. Lastly, the literature sources were fully read. Based on their content, it was decided whether they were to be included or not. Exclusion of records was done based on the following arguments:

- ⇒ The full article was not available through the used proxies.
- ⇒ The article consisted of a thesis.
- ⇒ The content of the article was out of the scope of this research.



**Figure 4.2 Search and Exclusion Process**

Despite adopting a rigorous approach to review the publications, there is still the risk of having overlooked important contributions by excluding cybersecurity maturity frameworks from the search because these could not produce measurable outputs to determine cybersecurity posture. Since the research field is still emergent in nature, it makes sense that results are currently ongoing in terms of research. However, assessing the quality of the frameworks and models-in-progress is an arduous and error-prone task. By limiting the review, there was a focus on mature research adhering to the high-quality standards and workflow dynamics of healthcare, which, in turn, ensures quality in the reported findings.

The subsequent sections discuss cloud security in general and, specifically, in healthcare. Afterwards, the challenges in maturity assessment of security in cloud-based healthcare, need for a cloud security maturity model in healthcare, and gaps in knowledge are identified. Lastly, publications about cybersecurity

standards and cloud security maturity models/metrics, in general and in healthcare, are reviewed.

## **4.2 Cloud Security**

Security is considered essential for cloud computing as a robust, feasible, and versatile solution. There is a vital concern about crucial security and legal challenges for cloud computing, including service availability, data confidentiality, provider lock-in, and reputation fate sharing. These concerns are not based only on existing problems directly inherited from adopted technologies but also on new problems derived from essential cloud computing features like scalability, resource sharing, and virtualisation. The difference between these features can be further distinguished by examining the definition of the essential cloud computing characteristics proposed by the National Institute of Standards and Technology (NIST) (Mell and Grance, 2011), which also introduces the service models for services (software as a service [SaaS], platform as a service [PaaS], and infrastructure as a service [IaaS]) and deployment (private, public, community, and hybrid).

Due to the ever-growing interest in cloud computing, there is an explicit and continuous effort to evaluate the current developments in security for such technology, considering both problems already identified and possible solutions. An authoritative reference in the area is the risk assessment developed by the European Network and Information Security Agency (ENISA) (Catteddu and Hogben, 2009). Not only does it list risks and vulnerabilities, but it also offers a survey of related works and research recommendations. Similar is the security guidance provided by the Cloud Security Alliance (CSA) (CSA, 2011), which

defines security domains congregating specific functional aspects, from governance and compliance to virtualisation and identity management. Mutually, these documents present a plethora of security concerns, best practises, and recommendations regarding all types of services models and possible problems related to cloud computing, from data privacy to infrastructural configuration.

Apart from the earlier mentioned references and top threat analysis—which highlights different security issues related to cloud computing that require further study to be appropriately addressed and, consequently, to enhance technology acceptance and adoption—there are several researchers and practitioners who have identified cloud threats, vulnerabilities, attacks, and other security and privacy issues. They have also provided countermeasures in the form of frameworks, strategies, recommendations, and Service-Oriented Architecture (SOA) (Khalil, Khreishah and Azeem, 2014; Veeramachaneni, 2015). Additionally, efforts in areas such as ad-hoc networks have been set to address the emerging security problems in the clouds and have addressed single attributes of cloud computing security such as data integrity, authentication vulnerabilities, and auditing (Khalil, Khreishah and Azeem, 2014; Subramanian and Jeyaraj, 2018).

Other authors discuss cloud security issues involving data, applications, and virtualisation (Mell and Grance, 2011) and present surveys on cloud security requirements such as confidentiality, integrity, transparency, availability, accountability, and assurance (Duncan and Whittington, 2014). A survey on the different security issues of the service delivery models of the cloud has been presented, and the security challenges specific to the public clouds are discussed

by several researchers (Jansen and Grance, 2011; Shin, Kobara and Imai, 2012). Classification and validation of the security issues and requirements in the cloud based on the SPI (SaaS, PaaS, IaaS) cloud infrastructure and services model are also discussed (Zissis and Lekkas, 2012; Hashizume *et al.*, 2013; Whaiduzzaman *et al.*, 2014). Albeit how valuable in successfully addressing cloud security issues, these studies must further understanding of the multiple security challenges in a holistic way and how they affect a particular environment. Thus, the next section investigates cloud security in healthcare.

### **4.3 Cloud Security in Healthcare**

According to the European Union (EU), eHealth refers to tools and services using information and communication technologies (ICTs) that can improve prevention, diagnosis, treatment, monitoring, and management of healthcare. This includes information and data sharing amongst patients and health service providers, hospitals, health professionals, and health information networks and of electronic health records; telemedicine services; portable patient-monitoring devices; operating-room scheduling software; robotised surgery (Kert, Markatos and Preneel, 2015). eHealth can benefit the entire community by improving access to care and quality of care and by making the health sector more efficient. ICT has been exploited in the healthcare sector for several decades. However, at present, there is the transition from the traditional model of a stand-alone health information systems (HIS), which is the HIS operating within the boundaries of a single healthcare organisation (HO), to the networked HIS that is an HO's HIS interconnected to HISs of other HOs or even of third parties, over national or international wide area networks (WANs). Moreover, web-based eHealth



services are already being regularly provided, and the healthcare sector has started utilising the cloud computing paradigm. Additionally, mobile devices like laptops, PDAs, and even mobile phones are being increasingly used by the healthcare sector to access, store, or transmit health information within the framework of providing health services. The trend towards seamless system and data interconnection, mobile services, smart devices, and data analytics has already started and will likely lead to revolutionary changes in the delivery of healthcare.

The security of health information and the privacy of the patients is a well-researched subject. A wealth of literature on this topic has been produced in the past decades. Issues that have been investigated for the present study pertain to the perceptions, attitudes, and concerns of healthcare service consumers regarding the privacy of health information subjects (Gaylin *et al.*, 2011; Ancker *et al.*, 2013). The perspectives of healthcare providers on the need for compliance to existing legal and regulatory requirements regarding the cybersecurity and privacy of health information, and technical and organisational methods for controlling access to online health information, have also been researched (Khan *et al.*, 2014). Furthermore, literature relating to health information cybersecurity and privacy on web-enabled healthcare platforms and health information security and privacy in the cloud computing paradigm were reviewed (Khan *et al.*, 2014; Das *et al.*, 2018). Last was the review of implications of privacy and security on healthcare practise and health information security-risk management (Youssef and Youssef, 2014; Masud and Hossain, 2018). A range of relevant standards of

different standardisation organisations has complemented these extensive research results.

However, despite the available technology, knowledge, and guidance, cloud security remains an issue in the healthcare sector. This is probably because, whilst most people recognise the need for securing healthcare cloud, what is often ignored is the fact that security provides technical solutions by creating physical and electronic barriers. The fundamental problems in computer security are no longer about technology but about applying that technology (Schneier, 2000) to the healthcare sector.

Despite the potential benefits of cloud computing in eHealth services, information security is still uncertain, and security problems have become more complex in the cloud models and require added effort to implement data management policies (Koo and Kim, 2015). The data stored in the cloud environment can be accessed or managed by more than one person (Rao and Selvamani, 2015), thus resulting in several major issues and concerns around data transmission and access control (Reddy, 2015). In addition, when users store and transfer their information on the cloud, the integrity of data and protection related to how to transfer healthcare data safely is an issue (Azhar *et al.*, 2014).

Another concern is that the storage of healthcare information in the cloud results in the patients losing physical control of their personal information. Transmission of data from one organisation to another is very delicate such that the patients must be vigilant in understanding the risks of data breaches in the new environment. To the best of the author's knowledge, there is currently no existing nameless and secure data exchange solution in the healthcare cloud

environment (Rahman *et al.*, 2016). Data stored in the cloud is often placed in a virtual environment, whose virtual server space could be shared with other customers of cloud service providers (CSPs). Healthcare organisations that transmit sensitive and regulated data into the cloud should ensure that the data is encrypted and secured.

In addition to concern about shared computing resources within cloud infrastructures is identity and access management. Cloud technology increases functionality and accessibility and introduces additional needs in terms of information security, particularly authentication. Authentication using widely documented PINs is designed as a solution to overcome the vital issues that are usable and secure through biometric-based techniques to user identity (Saevanee *et al.*, 2015). In the orthodox authentication method for access management, there might be an illicit use of data if the password is disclosed to an unauthorised person. Current identification and authentication methods in healthcare organisations may not be appropriate in cloud computing, and if these have a combination of single username/password for certain sensitive applications, they can present a weak link in the security structure.

In the cloud, identity management helps to maintain security, identification, and control and emphasises identity and access control. In another regard, the use of the Internet in healthcare services delivery equally provides vital benefits to providers and patients. However, unauthorised access to healthcare data in virtual environments may result in abuse of data and regulatory noncompliance. Therefore, use of the cloud in healthcare has led to the use cybernetics management solutions for the secure transmission of data, providing solutions

across broadband networks and protecting devices from data breaches and unauthorised access (Gunamalai and Sivasubramanian, 2015).

One of the most important changes in healthcare over the past two decades is the increasing investment in healthcare information security and confidentiality. Ensuring healthcare information security, privacy, and confidentiality is a continuous process and the serious responsibility of every healthcare organisation (Haufe, Dzombeta and Brandis, 2014). Cyberattacks and limited knowledge of authorised users are the main threats to healthcare systems. Cyber attackers use various means to breach confidentiality, integrity, and information accessibility, whilst users intentionally or through negligence can also be significant dangers to information security (Safa *et al.*, 2015).

For cyber attackers, the cloud platform produces more of a potential attack surface than a traditional data centre. Cyberattacks using malware infect healthcare systems' components and spread throughout the environment. Thus, protecting the healthcare cloud from malware and other security threats requires identity management at network boundaries to ensure that only authorised users have access to the system. The same is true for securing server and client platforms to ensure data integrity. This feature is a necessity for healthcare cloud computing, and integrity here refers to the fact that unauthorised user has not accessed healthcare information in cloud.

Hence, considering the extent of research already performed in the field, new research challenges primarily emerge because of the evolution of the healthcare system. At the same time, new computing paradigms and technological developments find their way into the healthcare sector. This implies that health

cloud security must be re-examined from a different perspective. The conditions under which new technological developments may be securely, effectively, and safely applied in the healthcare sector must be thoroughly investigated. Issues related to enabling secure eHealth services delivery and privacy-preserving information sharing over cloud platforms must be addressed and resolved. Lastly, a significant field of research is the preservation of security and privacy levels when interconnecting systems of varying degrees of maturity in the healthcare sector.

It is clear that the security is one of the most important issues in hindering cloud computing acceptance. Other issues such as identity management and access control for virtual cloud environment, authentication and authorisation, and cyberattacks are also major concerns. Putting one's data or running software on someone else's hard drive or using someone else's CPU may seem daunting to many, and most security challenges in cloud computing technology such as data mobility, multitenancy, and access control pose serious threats to sensitive information and software in healthcare organisations. Thus, all involved parties and their interactions in healthcare cloud computing should be defined and identified to ensure secure information exchange. Cloud service providers and healthcare organisations must establish clear processes for maintaining security in cloud environments. Protecting sensitive electronic medical data is one of the most essential responsibilities of healthcare organisations and one of the most tightly regulated areas in cloud. Thus, an essential procedure to improve security and deflect threats is through comprehensive understanding and the effective execution of dependent concerns and data protection (Mehraeen *et al.*, 2016).

#### **4.4 Cyber Security Standards, Best Practices, and Guidance**

Cyber security standards, guidance, and best practises have been in use, and their similarity is that they are reactive in nature. However, gaps exist between deciding whether something is needed and achieving implementation with such practises, which may span years. This becomes more of an issue for international standards due to the differing agendas of different countries, which can further increase the time to implementation. The problem is worse in a technological environment, such as security in computing, and especially in a fast-moving technology like cloud computing. However, not only is technology rapidly changing, but the threats to technology are also developing at a considerable pace (Cisco Annual Security Report, 2013).

The standards outlined in this research were reviewed because they are the industry frameworks that encompass the recently updated NHS National Data Guardian's (NDG) data security standards. The NDG data security standards are applied to every organisation handling health and social care information (NHS Digital, 2018). This research's comprehensive scope leverages standards as a reference in the maturity assessment process to build the proposed novel maturity model. The standards provides views into compliance with the industry requirements.

The International Organization for Standardization (ISO) 2700 series support healthcare organisations to drive real-life organisational improvement, as the standards are included in the healthcare organisation's existing policies, processes, and procedures. The USA-based National Institute of Standards and

Technology (NIST) Special Publication (SP) 800 series, NIST Cyber Security Framework (CSF), and Cloud Security Alliance Cloud Controls Matrix (CSA CCM) are frameworks that can be used to support data security and protection assurance in healthcare. When it comes to compliance for healthcare IT, the compliance rule comes from Health Insurance Portability and Accountability Act (HIPAA) as a prescriptive guidance. Health Information Trust Alliance (HITRUST) provides the assessment to demonstrate the compliance to standards such as HIPAA and Health Information Technology for Economic and Clinical Health (HITECH). It is relevant to mention that both NIST and HIPAA are United States specific.

#### **4.4.1 International Organisation for Standardisation (ISO)**

ISO 2700-series standards produced by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) provide best practises recommendations that cover the fundamental requirements of information security management systems as well as guidelines and principles for the implementation of such systems. The ISO 27001 (ISO/IEC 27001:2013 Information technology–Security techniques–Information security management systems–Requirements, 2013) is valid for all organisations, regardless of their size and industries. It specifies the method that organisations should use for information security and the essential components thereof. It also ensures that identification and management of risks are properly verified. Compliance to such standard saves organisations from financial penalties and losses associated with data breaches; helps with meeting business, legal,

contractual, and regulatory requirements; and protects and enhances their credibility and reputations.

ISO 17522 (ISO/TR 17522:2015, Health informatics—Provisions for health applications on mobile/smart devices, 2015) and ISO 27799 (ISO 27799:2016—Health informatics—Information security management in health using ISO/IEC 27002, 2016) standards are targeted towards health informatics. They provide guidelines for designing health-specific information management systems based on ISO 27002 and control patient safety within such systems, respectively. ISO 27001 can be integrated with ISO 27799 standards to address healthcare-specific risks. ISO 27017 (ISO/IEC 27017:2015—Information technology—Security techniques—Code of practise for information security controls based on ISO/IEC 27002 for cloud services, 2015) provides detailed guidance and recommendations for cloud adoption. ISO 22857 addresses the protection requirements to facilitate cross-border transfer of personal healthcare data (ISO 22857:2013—Health informatics—Guidelines on data protection to facilitate trans-border flows of personal health data, 2013).

Used together, these standards provide a complementary regimen for an organisation's cybersecurity readiness; however, navigating the many standards is complicated, has time and cost implications, and does not completely address some of the healthcare-specific concerns. Furthermore, some healthcare organisations have not been able to adapt the standards, guidelines, and best practises from the frameworks to their specific contexts and develop practises that meet their own needs. Other concerns include extensive time use and



expense of complying with different standards and the need for clarity and simplicity in implementation.

#### **4.4.2 Health Information Trust Alliance Common Security Framework (HITRUST CSF)**

Healthcare industry leaders have provided a harmonised, certifiable framework for all organisations that create, access, store, or exchange sensitive and/or regulated health data using HITRUST. The HITRUST Common Security Framework (CSF) version 9 (HITRUST CSF version 9.1, 2018) is a comprehensive, risk-oriented framework that normalises the cybersecurity requirements of healthcare organisations. It is based on federal legislation such as the Health Insurance Portability and Accountability Act (HIPAA) 164.502(ii) and globally recognised standards and guidance, including ISO 27799 using ISO 27002, NIST SP 800-53 r4 AC-19 (NIST Special Publication 800-53 Revision 4—Security and Privacy Controls for Federal Information Systems and Organizations, 2013). It provides scalable security requirements tailored to the needs of the healthcare organisations, allowing them to monitor and maintain compliance with HITRUST data security controls across their cloud infrastructure, including multi-cloud deployments.

The HITRUST framework's mapping with the NIST CSF reveals an industry-specific model implementation, whilst the NIST framework provides broad guidance for critical infrastructure industries on organisational-level risk programmes that are holistic and used across industries. However, a major

constraint for the HITRUST framework is that it is yet to receive worldwide acceptance.

#### **4.4.3 National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)**

In addressing cybersecurity, many entities both within and outside of the healthcare sector have voluntarily relied on detailed cybersecurity guidance and specific standards issued by the National Institute of Standards and Technology (NIST). NIST developed a set of guidelines on security and privacy in public cloud computing, SP 800-144 (Jansen and Grance, 2011). It provides an overview of the security and privacy challenges for public cloud computing and presents recommendations that organisations should consider when outsourcing data, applications, and infrastructure to a public cloud environment. NIST also developed a special publication, SP 800145 (Mell and Grance, 2011), for the definition of cloud computing, which has been globally accepted. The SP 500-299 framework (NIST Cloud Computing Security Working Group, 2013) was developed to identify a core set of security components that can be implemented in cloud to secure the environment, operations, and data migrated to the cloud. It also released SP 500-291 Cloud Computing Standards Roadmap (Hogan et al., 2011), SP 800-146 Cloud Computing Synopsis and Recommendations (Badger et al., 2012), and SP 500-292 Cloud Computing Reference Architecture (Liu et al., 2011). SP 800-66 (Scholl et al., 2008) was developed for guidance in IT security planning, implementation, management, and operation. It includes publications that address many security areas that are impacted by the HIPAA cybersecurity rules. NIST 800-66 provides guidance on how to map HIPAA

controls with NIST 800-53. This is the only guideline that is specifically focussed on healthcare, although it does not mention cloud computing.

In addition, to address the ever-increasing attacks on critical infrastructure, NIST also developed the cyber security framework (CSF) that provides a risk management model which various industries can leverage for improving the management of cybersecurity risk and achieving resilience; it was based on ISO 27001, Control Objectives for Information and Related Technology (COBIT) (A Business Framework for the Governance and Management of Enterprise IT, 2012), and NIST 800-53. The framework is designed to complement organisational security processes and facilitate privacy risk management consistent with an organisation's existing approach to cybersecurity. To ensure extensibility and enable technical innovation, the framework is technology neutral (NIST, 2017). This allows the relevant stakeholders to assess cybersecurity and identify gaps.

However, the shortfall of the framework's security controls was that they were specifically designed for US federal agencies and are not accepted worldwide. Initially, it was not sufficiently specific about cloud environments, but now major cloud service providers such as Amazon Web Services (Cotton et al., 2017) and Microsoft Azure ('Mapping Microsoft Cyber Offerings to NIST Cyber security Framework Subcategories', 2018) have taken steps to align their offerings to the framework, addressing the ambiguities about the use of the CSF in the cloud.

#### **4.4.4 Health Insurance Portability and Accountability Act (HIPAA)**

The HIPAA was developed to ensure security and privacy of individually identifiable health information. HIPAA deals with security and privacy through its privacy rule (The Privacy Rule–HIPAA, 2015) and security rule (The Security Rule–HIPAA, 2017). The privacy rule ensures the flow of health information needed for quality care by addressing proper use and disclosure of health information. The security rule aims at protecting the privacy of individuals' health information by adopting new technologies with a goal of achieving improved quality and efficiency of patient care. It operationalises the protection mechanisms contained in the privacy rule. HIPAA privacy and security rules are applied to healthcare providers and non-healthcare providers supporting healthcare providers holding or transmitting health information in electronic form. HIPAA compliance cannot be overlooked when it comes to cloud computing; however, it is no longer enough for a vendor to simply claim 'HIPAA readiness'. Its controls are indicated as required, which makes implementation unclear. HIPAA is also not 'certifiable', resulting in the need for healthcare organisations to perform self-assessment for compliance.

The scope of security and privacy protections available in HIPAA are extended through the Health Information Technology for Economic and Clinical Health Act (HITECH). In the healthcare industry, HITECH (HITECH Act Enforcement Interim Final Rule, 2017) provides legal liability for noncompliance to HIPAA and ensures the disclosure of breach and unauthorised use of electronic health records to necessary stakeholders.

#### **4.4.5 Cloud Security Alliance Standards Cloud Controls Matrix (CSA CCM)**

Cloud Security Alliance (CSA) and HITRUST developed security guidance for critical areas of focus in cloud computing, including various versions. Cloud Controls Matrix is a tool that maps security practises for the cloud with traditional security regulations and standards, such as Payment Card Industry (PCI), a MasterCard data security standard; HIPAA; and ISO 27000. Part of the mapping is achieved by leveraging the HITRUST Common Security Framework (CSF), a comprehensive security framework that provides prescriptive guidance and best practises and incorporates the existing security requirements of healthcare organisations, including federal (e.g., HIPAA and HITECH), third-party (e.g., Payment Card Industry (PCI) and COBIT), and governmental agencies (e.g., NIST). There are several versions: Version 1.0 (Security Guidance for Critical Areas of Focus in Cloud Computing, 2009), Version 2.1 (Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, 2009), Version 3.0 (Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, 2011), and Version 4.0 (Mogull et al., 2017). The latest version focusses on meeting the demand of security changes. It also introduces better standards for organisations to manage cybersecurity in cloud by implementing security domains. The guidance can be applied to a cloud service models (Infrastructure-, Platform-, Software – as a Service) and four deployment models (public, private, community, and hybrid cloud) with derivative variations that address specific requirements. The guidance also included thirteen different domains, which are divided into two general categories: governance and operations. The governance domains focus on broad and strategic issues as well as policies within a cloud

computing environment, whilst the operations domains focus on more tactical security concerns and implementation within the cloud architecture.

The Cloud Controls Matrix strengthens existing cloud information security by emphasising business information security control requirements, normalising cloud taxonomy, and encouraging consistent security measures. Regarding cloud security management, the guidance focusses on cloud-specific concerns: interoperability and portability, data security, and virtualisation. Dividing the implementation domains into two groups with strategic and tactical categories is another salient point provided by the guidance. This approach allows cloud consumers, providers to bring financial, and human resources into security consideration. Furthermore, the guidance can be mapped to existing security models, including the Cloud Control Matrix (Auditing the Cloud Controls Matrix, 2013).

Despite these benefits, the guidance lacks assessment standards for each domain. In addition, it does not consider metrics for security practises. Therefore, organisations find it difficult to determine the security level of a domain.

#### **4.4.6 Summary of Reviewed Standards**

The NIST cybersecurity framework provides a set of activities to aid healthcare organisations in developing their individual maturity profiles. Although this framework is robust, it relies on operators to voluntarily develop individual profiles for their organisations. The ISO standards, whilst offering more specific advice, are complicated to implement and do not specifically address mutually supporting healthcare organisations. Overall, the review of the cybersecurity standards

(Section 4.4) shows that either they are complicated to implement or the organisation's processes may need to be refined during implementation. These standards and guidelines are strongly complied with by industries, but as assessed based on their applicability to the domains in Table 4.1 they fall short of explicit application to healthcare cloud.

Next, there is a focus on mapping the reviewed standards to the standards' application domains. In this context, application domains refer to the suitable applicability of the standards of using these domain titles as measures: 'healthcare cyber security', 'cyber security', 'healthcare cloud security', 'cloud security', 'healthcare usability', and 'health informatics'.

Other characteristics to be included in the review are the relationships between the standards to reveal their interactions with other frameworks. It should be noted whether there is a framework to confirm compliance with the standard or, alternatively, whether or not it is common to have third-party audits certify compliance.

To address healthcare cloud security-specific needs, standards are based on parameters such as scope, level of integration, industry applicability, prescriptiveness, scaling, tailoring, compliance, certification, shared assurance, assessment guidance, and tool support. With these aspects as a guide, the following section reviews cloud security maturity models in eHealth.

Standards	Application domain	Interaction with other frameworks	Certification/audit
ISO 2700 series	Cloud security	ISO 27001/2, 27799, 27017	Audits of compliance to the standard are performed, and certification frameworks exist.
HITRUST CSF	Health informatics	HIPAA 164.502(ii), ISO 27799, NIST CSF	Audits of compliance to the standard are performed, and certification frameworks exist.
NIST CSF	Cyber security, cloud security	ISO 27001, HIPAA, COBIT	Audits of compliance to the standard are performed, and certification frameworks exist.
HIPAA/HITECH	Health informatics	HITECH	The only way to prove compliance is through an external audit.
CSA CCM	Cloud security, cyber security	HITRUST, CSA standards	Audits of compliance to the standard are performed, and certification frameworks exist.

**Table 4.1 Summary of reviewed standards**

#### **4.5 Comparison of Maturity Models Applicable in Healthcare**

The comparison of maturity models applicable in healthcare identifies and compares existing cyber security/capability maturity models to provide a summary of the best practices. Based on the inclusion criteria, a search statement is formulated as defined in Section 4.1.1. To ensure all the maturity models compared are rooted in well-structured concept, exclusion criteria is developed as defined in Section 4.1.1.



The cybersecurity maturity models identified and reviewed are included because they outline different stages that show maturities in cyber security capabilities or processes. Secondly, the areas in which the models are used include healthcare or cyber/cloud security, capability maturity model in electronic healthcare, or a combination of both. The maturity models are compared to identify relevant theoretical structures and content. The comparison criteria include the dimensions (such as maturity levels and domains) in the maturity models are compared to identify relevant maturity structures. Lastly, the relevant content of the maturity models are identified.

These cybersecurity maturity models were also chosen for this study because of their main design features. National Healthcare Service Infrastructure Maturity Model (NHS NIMM) is applicable to the healthcare organisational structure, culture, and working practises, aligning the strategic and tactical priorities of the organisation. It is also independent of technology and considers both technical and business capabilities of IT infrastructure. Health Information Network Capability Maturity Model (HIN CMM) can be used for intra-organisational and interorganisational benchmarks and assessment and organisational learning amongst healthcare institutions in a physical jurisdiction. The Information Security Focus Area Maturity Model (ISFAM) is easy to extend according to changes in an organisation's IS needs and priorities. For the most part, these models are easy and intuitive to use and are written without excessive technical jargon. These models are considered the theoretical foundations for the development of the proposed maturity model M<sup>2</sup>HCS (discussed in Chapter Five).

#### **4.5.1 Information Security Focus Area Maturity Model**

The Information Security Focus Area Maturity (ISFAM) model is a focus area-oriented maturity model, originally proposed as a method for incremental progression (Steenbergen et al., 2010). It consists of a fixed number of maturity levels; each process identified by a focus area/domain is assigned its own number of progressively more mature capabilities. It consists of four focus area groups, which cluster 13 focus areas and distribute 51 capabilities over 12 maturity levels. The last can be grouped, in turn, for convenience into four maturity stages, which strongly resembles the audit control pattern (Singleton, 2009). The overarching 12 levels result automatically from the capability interdependencies (Steenbergen et al., 2010).

The model's underlying assessment consists of a series of 161 yes/no questions. The assessment of the maturity level is executed through a survey or a directed interview with an expert. The ISFAM covers the complete domain of information security, combining the application of information security framework (ISO-light), ISO 2700-series, the Certified Information Systems Security Professional (CISSP) course, Standard of Good Practise of the Information Security Forum (ISF), and the International Business Machines Corporation (IBM) Security Framework (Spruit and Röling, 2014).

As with all focus-area maturity matrices, the lowest implemented capability defines the maturity level reached. ISFAM was successfully evaluated using a medium-sized telecommunications organisation and a small or medium-sized enterprise (SME) in the healthcare sector. Despite that, it is extensive, relatively

fine-grained, and practical approaches are based on IBM's experiences, the ISFAM model must redefine the capabilities' improvement actions by making them less simplistic. It also does not mention being applicable to technologies such as cloud computing.

#### **4.5.2 Cloud Security Capability Maturity Model**

The Cloud Security Capability Maturity Model (CSCMM) includes domains and maturity levels. There are twelve cloud security domains and four maturity levels. Each domain consists of a set of cybersecurity practises which are achievement objectives-specific for each cloud security domain. The maturity levels apply to each domain and specify progression of maturity. The model can be tailored for suitable objectives of different cloud service models (IPSaaS) and deployments (public, private, and hybrid cloud). Lastly, it provides the tool for organisations to implement and enhance their cybersecurity capabilities on the cloud system (Le and Hoang, 2017).

There is not a complete cloud security standard because cloud technology is evolving much faster than standards are (Duncan and Whittington, 2014). Therefore, creating a set of cybersecurity domains just based on the current security standards does not fully consider emerging issues and attack surfaces. Cloud Security Capability Maturity Model (CSCMM) was built from a systematic review approach on existing cloud security models and standards, traditional security maturity models, and trends in emerging technologies. As a result, these twelve security domains—eight are from traditional maturity models, and four are

cloud specific—cover comprehensive aspects of cybersecurity and accommodate emerging security issues.

To assess the maturity level of the model in general and a security domain in particular, a security metrics framework was proposed. This framework includes relevant quantitative metrics for measurable assessment. It presents a balance assessment of the overall security of an organisation, both qualitatively and quantitatively. For senior managers, it offers assessment of the security status for making decisions concerning business plans and direction. For security practitioners, it offers proactive measures and responsive actions. In addition, the CCSMM model has three dimensions—domain, level, and community (such as organisation, community, and state)—which makes the model more suitable for organisations of different sizes. However, this model is considered technically complex to implement in healthcare (Siponen and Willison, 2009; Stevanović, 2011; Le and Hoang, 2016).

#### **4.5.3 NHS National Infrastructure Maturity Model**

The National Infrastructure Maturity Model (NIMM), a maturity assessment framework designed by Connecting for Health (CfH), has provided useful guidance, national standards, best practises, and capability maturity tools for the NHS IT organisations to benchmark their local IT infrastructure services/capability and create a road map for improvements. It helps NHS IT organisations to carry out an objective self-assessment of the current IT infrastructure to assess their current 'point in time' maturity of specific

infrastructure capabilities and identify infrastructure maturity improvement projects.

The NIMM framework is split into 13 categories across technical and business areas, 74 capabilities, 5 perspectives, and a number of key performance indicators. Its two main tools are the capability assessment documents, which contain key performance indicators (KPIs) for assessing each capability, resulting in a 'point in time' maturity score, and key capabilities self-assessment spreadsheet, which is a dashboard spreadsheet that records the scores from the capability assessments on a scale from 1 to 5, where 5 is the most mature; it also gives an overview of assessment progress (NHS, 2011a).

Each category is further divided into a number of capabilities used to target the assessment to a specific area. A capability is then further organised into perspectives. Each perspective has a number of KPIs associated with it, against which the capability in question is assessed. Organising the metrics into perspectives provides the opportunity to review the capabilities 'in the round' and to develop an overall view of the capability rather than just from a technology viewpoint.

The NHS Infrastructure Maturity Model (NIMM) provides a consistent framework for organisations to measure their own capabilities in specific areas and to subsequently identify and prioritise activity. Trusts/organisations create their own local assessments, aligned with NIMM, to support their local IT maturity assessment efforts. This approach ensures that Key Performance Indices (KPIs) and metrics reflect achievable maturity levels within the NHS. Not all capabilities

must be completed at once. Users can review the capability list, decide the priorities for their IT organisation, and concentrate their efforts on completing this subset.

NHS IT organisations are to exercise the 12 NIMM core capability assessments first. Afterwards, a road map should be formulated to improve maturity. Then assessments that are more specific to the healthcare organisation should be selected and completed, and the outputs from these are incorporated into the formulated road map (Savvides, 2009). Most healthcare trusts are required to work towards level 3, increasing the maturity of their infrastructure and service provision and moving from manual configurations to managed systems with automation and proactive monitoring of services. The healthcare organisations generally recognise the fundamental part played by infrastructure in underpinning all information management and technology (IM&T) strategy, and so they have adopted the NIMM (NHS England, 2014).

This model is still presently relevant in the cybersecurity maturity assessment of NHS IT organisations and is platform-independent; however, it does not consider the rapidly changing landscape of technology and security, such as cloud and its resulting threats.

#### **4.5.4 Health Information Network Capability Maturity Model**

The Health Information Network (HIN) Capability Maturity Model is a tool that supports objective self-assessment and formulates plans to improve operational capabilities, level of service, and value delivered by HIN organisations. This fully vetted and accepted pan-Canadian model serves as a strategic and operational

planning tool. It provides a tool which HIN planners and operators can use to conduct a stepwise assessment such as ascertaining a jurisdiction's HIN current capability maturity level, identifying a target maturity level appropriate to their needs, and developing a road map for moving toward that desired maturity level. It is based on other maturity models in healthcare and other industries, Canada Health Infoway's strategic opportunities for action and key enablers, HIN Planning and Operations Leading Practices Discovery Framework, and observations and input from interviews with the leading practise organisations. This model was also developed to aid in continuous planning and assessment.

The HIN Capability Maturity Model comprises ten capability domains and five maturity levels for each. It also includes an aggregate maturity across all domains, which can be used to broadly compare and communicate the overall maturity of the HIN. To apply this model, it must be refined with input from current jurisdictional HIE organisation operators, system planners, and policy makers, and tools for self-assessment, action planning, and progress monitoring are required to make it consistently and uniformly applicable (Giokas, Sekhon, Mestre, Geffen, Nouri, and Twoekowski, 2015). However, its shortcomings are in line with the NHS Infrastructure Maturity Model.

#### **4.5.5 Summary and Analysis of Reviewed Maturity Models**

Cloud security maturity models show the level of completeness of cyber and cloud security capabilities. Their key features are maturity levels (also known as security measurement scale), security domains (known as the logical groups of practises and processes), attributes (or core contents of the model), assessment

metrics for measurement, and road maps to guide improvement efforts. Their main functions are to assess healthcare cybersecurity performance in cloud and guidance for improvement of processes and practises.

The Cloud Security Maturity Model for healthcare is important because it provides a clear path to security in the cloud for healthcare organisations. Security threats in the cloud must be taken seriously; where there is no longer a defined perimeter and the attack surface is multiplied, attacks are more prevalent and pervasive. Considering the sensitivity of patients' data handled in healthcare organisations, there is a need to be proactive, and the best way to do so is extending cybersecurity in the processes and practises to include workflow in the cloud.

The twelve cybersecurity maturity models were reviewed to investigate their strengths and weaknesses. The similarities identified amongst these maturity models are that they are all multidimensional, including security domains and maturity levels. Most security domains vary from infrastructures, data, networks, humans, applications, and communications to compliance, legal, and contractual. Thus, to implement best security practises, standards such as National Institute of Standards and Technology (NIST) and the Information Standards Organization (ISO) 27000 series are the baseline to measure security levels in all models.

Most of the models have implementation process through four steps, from validation, and gap identification to priority and planning and plan implementation. Most of the models also implement a five-level framework to assess the security state of each domain. These five levels involve a three-stage process; the first stage is with no security management implementation. The following stage



focusses on the implementation of security standards to control security concerns. The third stage is an automatic security management with full security implementation; this is considered the innovative stage with highest security.

The differences identified include that each model has domains with various security requirements based on the goals of the model, giving each one different advantages. None of these models mentioned extends its application to cloud computing environments and were industry-generic, not streamlined to healthcare environment.

Information Security Focus Area Maturity Model (ISFAM) has successfully and conclusively been evaluated using a medium-sized telecommunications organisation. However, it does not mention being applicable to emerging technologies or cloud computing. Apart from the lack of validation of the real-life application of Capability Maturity Model and Metrics Framework for Cyber Cloud Security (CSCMM), its application to assess healthcare organisations would likely result in domain-specific challenges encountered when mapping the healthcare-specific processes to the CSCMM process areas. This is due to its strong prescriptive properties and detailed appraisals of the processes with respect to the requirements of the maturity levels. Thus, the use of CSCMM with a compatible, domain-specific model is suggested.

NIMM and Health Information Network Capability Maturity Model (HIN CMM) are nationally focussed maturity models. They are actively used and applicable within the United Kingdom and Canada, respectively. In addition, they are intended for determining the current capability of IT infrastructure within their local health

jurisdictions' current capability and setting future priorities. They are aim to enhance the overall IT management processes, access, quality, cost, and productivity of healthcare planning and delivery. However, NIMM is intended as a tool to identify its priority elements of IT infrastructure for assessment. While HIN CMM is intended as a tool for guiding stepwise assessment.

Furthermore, NIMM can be used for self-assessment and uniform application, without the support of any other tools. HIN CMM requires tools for self-assessment, action planning and progress monitoring to make it consistently and uniformly applicable. In addition, HIN CMM requires refinement with key stakeholders' input for its active use and application. NIMM is used to certify ICT infrastructure providers, while the HIN CMM supports policies that support creation of HINs.

Both models are presently relevant in the cybersecurity maturity assessment of healthcare organisations and are technology and vendor independent. NIMM focusses on NHS needs, whilst HIN emphasises jurisdiction's needs. However, neither considers the rapidly changing landscape of technology, such as characteristics of cloud computing and its resulting security threats.

Maturity Models	Dimensions	Assessment Metrics
ISFAM	12 maturity levels, 13 domains, 64 capabilities	A survey or directed interview
CSCMM	12 domains, 4 maturity levels	A security metrics framework
NHS NIMM	13 categories, 5 maturity levels, 74 capabilities	Balanced scorecards, dashboard
HIN CMM	10 domains, 5 maturity levels	Input from policy makers

**Table 4.2 Summary of reviewed maturity models**

## **4.6 Identified Research Gaps and Operational Characteristics of Proposed Model**

Apart from the lack of a security maturity model streamlined for eHealth cloud, the other identified gaps in the review of these maturity models occur in the aspect of adoption; the maturity models are either too complicated to implement, or they require the healthcare organisation's processes to be refined to suit their implementation. The review of these models results in the question: How can the adoption of the proposed model, Maturity Model for Healthcare Cloud Security (M<sup>2</sup>HCS), be increased effectively in the eHealth cloud environment?

The five factors of diffusion of innovation theory that impact adoption are the value the innovation provides over the current method, how easy it is for the innovation to be incorporated into healthcare organisational workflow, how easy to use the innovation is, how easy it is to try the innovation without commitment, and how visible the innovation is in the community of the adopter's peers (Sanson-Fisher, 2014).

In relation to this theory, the novel maturity model M<sup>2</sup>HCS seeks to achieve these operational characteristics (OC):

- ⇒ The M<sup>2</sup>HCS can support in the assessment of security practises in the eHealth cloud (OC1).
- ⇒ The maturity assessment metrics can be followed easily and intuitively (OC2).

- ⇒ The descriptions of the objectives are clear and relate to the maturity levels (OC3).
- ⇒ M<sup>2</sup>HCS supports the assessment of the maturity of each of the specified domains to identify weak and strong practises (OC4).
- ⇒ M<sup>2</sup>HCS can aggregate results from the individual domains to a suitable output that can be understood by all stakeholders (OC5).
- ⇒ Further steps towards improving the maturity level are recommended (OC6). Recommendations must be prioritised for improving the maturity based on available organisational resources (OC7).

M<sup>2</sup>HCS seeks to be a novel maturity model that satisfies these operational characteristics and assesses the security practises of a healthcare organisation using eHealth cloud. It also incorporates 'usability and functionality' objectives into its assessment of security practises. The fundamental reason for this addition to the proposed maturity model of M<sup>2</sup>HCS was that poor usability often equals poor security (Sheng *et al.*, 2006). Whilst much of the healthcare industry's discussion about usability seems to place emphasis on patients, in the proposed model, the focus is on gaining a better understanding of the needs, goals, and frustrations of stakeholders like physicians and other nonclinical staff. The inspirational frameworks for the usability and functionality objectives are the ISO 9241-11 (Bevan and Nigel, 2006; Bevan, 2009; Bevan, Carter and Harker, 2015) and Healthcare Information and Management Systems Society (HIMSS) Usability Maturity Model (Staggers *et al.*, 2011).

There are several approaches to perform healthcare workflows when using entirely different security mechanisms, and some are more secure than others. Practitioners select the more secure approach if it is easy to follow and allows them to complete their tasks quickly. However, if the more secure way is challenging, time-consuming, or stops them completing their tasks, then practitioners will expectedly find their own approach to get their tasks completed, but they may not use the more secure approach (Adams and Sasse, 1999). Scenarios like this depict how 'people often represent the weakest link in cyber security chain and are chronically responsible for the failure of security systems' (Schneier, 2000). However, if the appropriate security approaches for completing tasks or clinical workflows means that healthcare efficiency is reduced, medical practitioners seek to pursue other means.

The proposed model, Maturity Model for Healthcare Cloud Security (M<sup>2</sup>HCS), aims to assess the 'usability and functionality' objectives by focussing on transferring the effort of making security decisions away from end users (medical practitioners) and to the back end (server-side). Secondly, it aims to significantly improve security mechanisms by making them more usable, meaning security processes do not inhibit their clinical workflow. Thirdly, practitioners should be able to locate the right security advice and information when they need it, at the right times, supported by the right skills, tools, habits, and motivation. Overall, this model enhances the integration of security practises (some of which are taken from the models reviewed above) into healthcare administrative processes and daily workflows.

Usability is of great importance in healthcare because the effectiveness and efficiency of healthcare service delivery impact people's lives. The care and upkeep of patients' health are subject to effective healthcare efficiently delivered by practitioners. A more usable healthcare cloud improves patient safety, makes practitioners more content with their capability to provide care, and saves money.

#### **4.7 Chapter Conclusion**

This chapter reviews cybersecurity standards, best practises and guidance, and models including cloud security models and cybersecurity capability maturity models, mostly applicable within the healthcare environment. However, three specific issues must be addressed by the proposed model:

- ⇒ The influencing factors of cybersecurity on a security maturity model should be more than standards compliance.
- ⇒ It must integrate identified relevant factors into the maturity levels and determine appropriate metrics for security assessment.
- ⇒ The model should be malleable for ensuring current cybersecurity and extensible for dealing with security against emerging cyber threats.

The main insight obtained from the review is the present inadequacy of cybersecurity maturity models to effectively assess security in healthcare organisations which are actively using cloud computing. The reviewed existing maturity models do not focus on security for eHealth cloud services, which forms the purpose for the model proposed in this research.

By identifying interactions between the several domains of healthcare information security and signifying them cogently in the proposal of a Maturity Model for Healthcare Cloud Security (M<sup>2</sup>HCS), the aim is to mitigate reactive assessment of security in a healthcare cloud environment and support incremental operations to improve information security maturity within healthcare organisations. The following chapter discusses in more detail the design and development of the proposed maturity model (M<sup>2</sup>HCS).

## **Chapter Five**

### **5 Maturity Model Development**

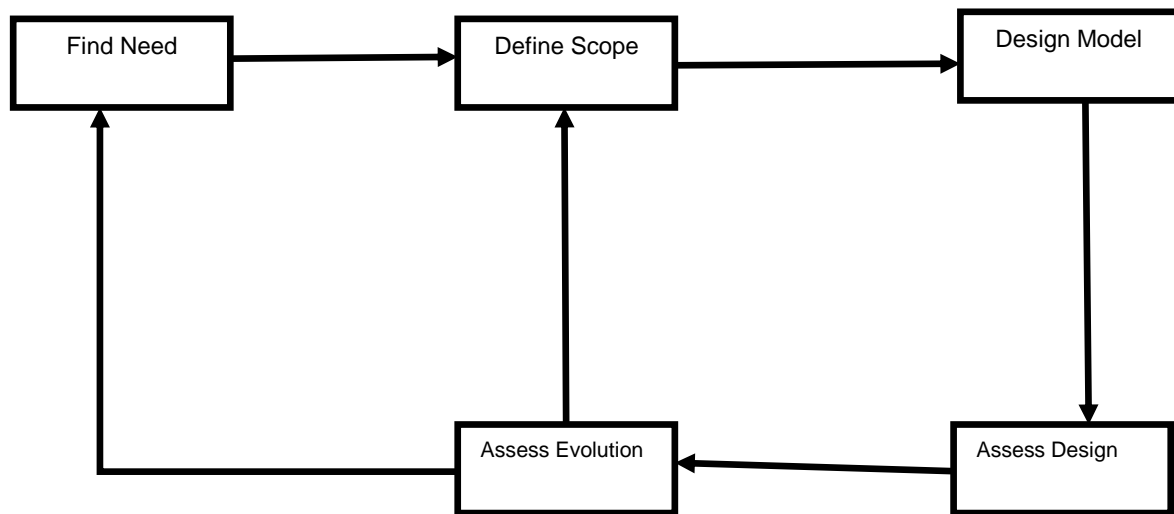
This chapter discusses the development process of the maturity model and the results of the survey feedback. It starts with a summary of the relevant theoretical background, and then the development strategy and approach are elaborated upon; finally, the results of the maturity levels and maturity dimensions are presented, leading to the maturity model, M<sup>2</sup>HCS. The methodology chosen was Design Science Research Methodology (DSRM).

#### **5.1 M<sup>2</sup>HCS Development Methodology**

A relative study was performed on the procedural methods used in the development of information system maturity models found in the literature (Becker et al. 2009, Bruin et al. 2005, Mettler and Rohner 2009). The foremost method used is DSRM (Hevner *et al.*, 2004; Elmaallam and Kriouile, 2013). In this research, it is essential to reflect the iterative stages which are, to clearly describe the structure of the maturity model, and validate the maturity model's capacity to solve the problem addressed (March and Smith, 1995). Hence, a robust and documented research method, such as DSRM, is vital for the development of Maturity Model for Healthcare Cloud Security (M<sup>2</sup>HCS).

DSRM presents the decision parameter elements (Figure 5.1). This method consists of five steps. Within each step, several decisions must be made before continuing with the process.





**Figure 5.1 Mettler Methodology Decision Parameters (Carvalho et al., 2017)**

⇒ **Recognise Need**

This is the first step, and two main parameters to deliberate on are the novelty and the innovation of the maturity model since this decides the need for this model. The novelty parameter assesses the security of healthcare organisations actively using cloud computing. This model considers the domain, controls, maturity levels, and assessment proven by theoretical conventions. Innovation is the second parameter considered for the development of M<sup>2</sup>HCS, which is a completely new model, not a variant or version of an existing one.

### ⇒ **Define Scope**

For the scope of this model, it must be determined if it focusses on a broad or specific area. Though a key feature of M<sup>2</sup>HCS is its inclusive nature, this model is applied solely to hospital organisations actively using cloud computing; for this cause, the research focusses on a specific area. Following this, the conditions and details must be reflected. Thus, M<sup>2</sup>HCS includes features related to the internal processes of healthcare organisations and the practises of their service providers. In accordance with the constituent directives of DSRM (Hevner *et al.*, 2004), the potential audience of the model should also be decided. For M<sup>2</sup>HCS, the choice of the audience parameter is the 'both' option to include the managers of the healthcare organisations who have the authority to make decisions (such as executives) and department directors (CIOs or IT directors).

### ⇒ **Model Design**

In this step, the model is constructed. This begins with the definition of the maturity concept of the proposed model. There are three different concepts of maturity (Mettler and Rohner, 2009), depending on whether its focus is on the process, the object, or the people. M<sup>2</sup>HCS uses the 'combination' approach to measure maturity as this increases the competence of healthcare cloud security (process oriented) and the approval of practitioners who use it (people oriented). In addition, M<sup>2</sup>HCS assesses the different controls concerning organisational and technical capacities. Whilst defining the maturity of the model, how maturity will

progress is also implicitly defined. Competence is often the fundamental objective of the processes and approval of practitioners a fundamental objective of the end users.

A maturity model can have multiple elements, as is the case with M<sup>2</sup>HCS. Therefore, it is important to decide if the advancement of maturity will be one-dimensional (only focussing on an aspect of security) or multidimensional (aiming at several aspects of security) (De Bruin *et al.*, 2005). The multidimensional maturity advancement of M<sup>2</sup>HCS is reflected by the aspects measured for maturity, encompassing comprehensive controls that measure the overall maturity of the healthcare cloud security and also the maturity of each domain of controls. Subsequently, M<sup>2</sup>HCS adopts the theory-driven knowledge base to develop maturity levels and take on a healthcare domain-specific metric. Furthermore, the format of the model is manual and specialised as an assessment tool of maturity for healthcare cloud security, and included is the textual description of its application. The choice of application means that data collection is based on self-assessment. Primarily, the managers of the healthcare departments, whose maturity is to be assessed, are the ones who must apply M<sup>2</sup>HCS since they know the reality of their organisation. Whilst the data collection process is fundamentally performed by the managers, it also includes other professionals in the organisation, such as technology practitioners.

### ⇒ Assess Design

This step is concerned with the validation of M<sup>2</sup>HCS. Validation, in this case, is the degree to which a maturity model is a precise demonstration of the real world from the viewpoint of the intended users of the model (Conwell, Rosemary and Marcia, 2000). Therefore, it is vital to define an approach to test the model after the development but prior to implementation. M<sup>2</sup>HCS has been validated in terms of form and content, using a case study and expert survey. This was based on extracting the experience and reflection of end users of the model. Care was taken to ensure that the ten experts have significant experience in security maturity assessment in a healthcare environment.

### ⇒ Assess Evolution

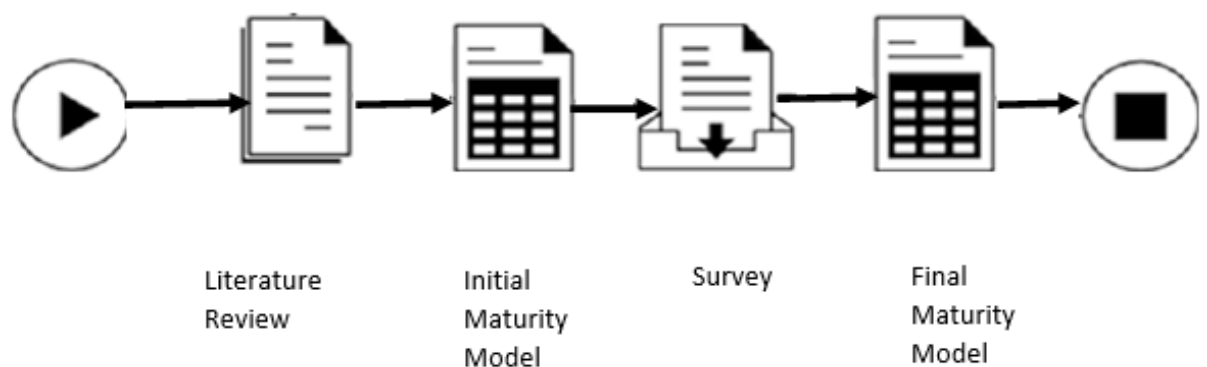
In this last step, the tendency of M<sup>2</sup>HCS to change over time was decided. This refers to the modification of the requirements to reach a certain level of maturity due to the innovation of new and better practises and technologies. Changes in the form and function of the model may be required to ensure its standardisation and global acceptance. (In this research, this step was not performed due to time constraints.) In **Error! Reference source not found.**, the chosen characteristics (underlined cells) are presented.

Design activities	Decision parameter	Characteristics			
1. Find Need	Novelty	<u>Emerging</u>	Pacing	Disruptive	Mature
	Innovation	<u>New</u>	Variant	Version	
2. Define Scope	Breadth	Generic issue		<u>Specific issue</u>	
	Depth	Individual/group	<u>Organisation</u>	Inter-organization	Global
	Audience	Management	Technology	<u>Both</u>	
3. Model Design	Maturity concept	Process	Object	People	<u>Combination</u>
	Goal function	Single dimensional		<u>Multidimensional</u>	
	Design process	<u>Literature</u>	Practitioner	Combination	
	Design product	Description of form	<u>Description of form and function</u>	Software	Combination
	Application method	<u>Self-assessment</u>	Third party	Experts	
	Respondents	Managers	Staff	Partners	<u>Combination</u>
4. Assess Design	Subject of validation	Process	<u>Product</u>	Both	
	Point of time	<u>Ex ante</u>	Ex post	Both	
	Validation method	<u>Natural</u>	Artificial	Both	

**Table 5.1 Decisions taken for the design of M2HCS (Mettler and Rohner, 2009)**

## M<sup>2</sup>HCS Development Process

The review of the relevant maturity models resulted in the identification of important domains and controls within Maturity Model for Healthcare Cloud Security (M<sup>2</sup>HCS). An overview of these identifications is presented below. A group of activities based on established research methodologies and considered most suitable for M<sup>2</sup>HCS was defined (Figure 5.2). The review of key concepts on healthcare cyber and cloud security maturity models was followed by the identification of domains, controls within the domains, levels, and validation of M<sup>2</sup>HCS. Based on the questionnaire survey of six field-related experts, M<sup>2</sup>HCS was validated. The chosen methodology, DSRM, supported these activities.



**Figure 5.2 Activities for the development of M<sup>2</sup>HCS**

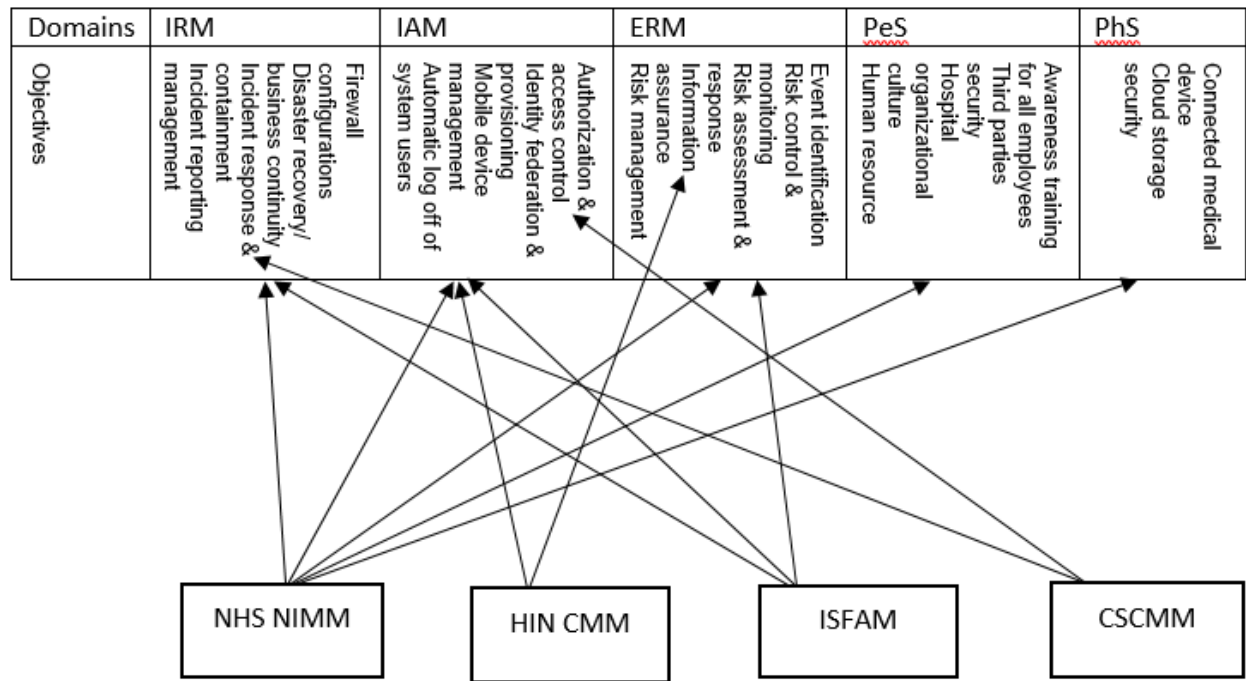
### 5.2 M<sup>2</sup>HCS Maturity Model

M<sup>2</sup>HCS combines its foundational models' capabilities to produce a more holistic model that can be used to develop a healthcare organisation's security practises against cyber and cloud security attacks. Its novel contribution lies in supporting healthcare organisations with developing the maturity of their security practises against emerging cyber and cloud security attacks.

Furthermore, it aims to assess the usability and functionality of the implemented security practises within each domain and the workflow of the healthcare organisation. The model is conceptualised at a high level, focussing on the characterisation of the maturity goals of cybersecurity for the healthcare organisation using third-party or their own cloud services. It bridges the gaps between the levels of governance and operation for healthcare at the maturity, usability, and functionality levels of their cloud cybersecurity capabilities. The model allows the assessment of present cybersecurity abilities and defines the main actions each healthcare organisation must perform to progress to the optimisation stage.

#### **5.2.1 M<sup>2</sup>HCS Maturity Domains**

Five security domains with frequent recurrence (incident response management [IRM], identity and access management [IAM], enterprise risk management [ERM], personnel security [PeS], and physical security [PhS]) were identified in the reviewed models (Figure 5.3). Each domain is a group of related cybersecurity activities that also focusses on aspects of cloud characteristics. The controls within each domain are the defined maturity goals specific for cloud cybersecurity. The domains are based on the categories of cybersecurity capability from the reviewed models. These five cybersecurity domains address comprehensive features of cloud security.



**Figure 5.3 Influences of Foundational Models and Development of Maturity Domains**

The IAM (Identity & Access Management) domain of the research model was mainly influenced by the HIN CMM (Health Information Network Capability Maturity Model), NHS NIMM (NHS Infrastructure Maturity Model), and ISFAM (Information Security Focus Area Maturity Model). Its objective—authorization and access control—was further influenced by the CSCMM. The IRM (Incident & Response Management) domain was mainly influenced by the NHS NIMM and ISFAM. Its objective—incident response and containment—was influenced by the CSCMM (Capability Maturity Model and Metrics Framework for Cyber Cloud Security) (Le and Hoang, 2017). The third domain, ERM (Enterprise Risk Management), was mainly influenced by the ISFAM (Spruit and Röling, 2014). Its objective—information assurance—was influenced by the HIN CMM (Giokas, Sekhon, Mestre, Geffen, Nouri and Twoekowski, 2015). The PeS (Personnel



Security) and PhS (Physical Security) domains were mainly influenced by the NHS NIMM (Savvides, 2009; NHS, 2011a).

Furthermore, the Healthcare Information and Management Systems Society's (HIMSS) cloud computing security in healthcare toolkit (HIMSS, 2017) supports the objectives of identity management and federation, business continuity and resiliency, incident response, and infrastructure security. The Cloud Security Alliance Cloud Control Matrix (CSA, 2017) also supports business continuity management, data centre security, governance and risk management, human resources, identity and access management, and incident management. Not included in Figure 5.3 is the objective of usability and functionality in each domain, which was mainly influenced by the HIMSS usability maturity model (Staggers *et al.*, 2011).

However, NHS Infrastructure Maturity Model is the main influence on Maturity Model for Healthcare Cloud Security as four domains were impacted by it (Figure 5.3). Since NIMM is a capability maturity model specific to UK healthcare organisations, it considers the processes implemented within the healthcare sector, thereby supporting the capability of M<sup>2</sup>HCS within the same sector. M<sup>2</sup>HCS combines ISFAM and CSCMM models that cover the holistic categories of cyber and cloud security domains, and it is streamlined to enhance the healthcare capability processes of the HIN capability maturity model and NIMM.

The proposed M<sup>2</sup>HCS model has two dimensions: maturity domains and maturity levels (Sections 5.2.1 and 5.2.2). The first dimension offers five cloud security domains. The maturity model also includes 20 objectives corresponding to each

domain (Section 5.2). Healthcare organisations can use these maturity levels to define their present maturity levels, decide their subsequent practicable maturity level, and detect the elements that must be satisfied to reach the next maturity level. The domains are:

- ⇒ Identity and Access Management (IAM): This guarantees verification, approval, and management of identities. The core focusses on identity verification—permitting an apt level of access—and policy administrations. This domain seeks to inhibit unapproved admission to physical and virtual resources.
- ⇒ Incident and Response Management (IRM): This focusses on incident identification, response, and management. Its major concerns include creating and conserving strategies, measures, and tools to identify, evaluate, and respond to cloud security incidents.
- ⇒ Enterprise Risk Management (ERM): This is another significant aspect of information security. A business may not always be secure, but it is capable of managing its risks. It is concerned about detecting potential breaches, preventing, and managing them: indemnification, mitigation, and retention.
- ⇒ Personnel Management (PeS): This emphasises human resource processes: pre-employment and employment through to termination. This ensures that the effective policies and procedures are in place to address security issues. It also supports an ethos of security and the constant suitability and attitude of all personnel.

⇒ Physical Security (PhS): This encompasses the devices and facilities of the cloud service provider and customer. The organisation must obtain a guarantee from the provider that suitable security controls are in position. It safeguards against environmental or other possible intimidations that could interrupt cloud services, devices, security controls, and backup utilities.

Interoperability and portability, virtualisation, and isolation could be added to create new domains, but these were not used in the proposed model. This is because there have been more recent attacks on the virtualisation layer, and isolation techniques have materialised as a new tactic for safeguarding cloud (Sonehara, Echizen and Wohlgemuth, 2011).

<b>Maturity Levels</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>
<b>Maturity Domains</b>	<b>Objectives</b>			
<b>Incident Response Management (IRM)</b>	Firewall configurations, data governance (IRM.1), disaster recovery, incident reporting and response (IRM.2), usability and functionality			
<b>Identity and Access Management (IAM)</b>	Authorisation and access control (IAM.2), mobile device management, Identity federation and provisioning (IAM.1), account lockout procedures, usability and functionality			
<b>Enterprise Risk Management (ERM)</b>	Threat and vulnerability awareness, risk identification, risk control and monitoring (ERM.1), risk assessment and response (ERM.2), usability and functionality			
<b>Personnel Security (PeS)</b>	Employee training (PeS.1), external personnel security, organisational culture (PeS.2), usability and functionality			
<b>Physical Security (PhS)</b>	Connected medical device (PhS.1), cloud storage security (PhS.2), usability and functionality			

**Table 5.2 Dimensions of M2HCS**

### 5.2.2 M<sup>2</sup>HCS Maturity Levels

This overall framework is proposed as a tool to assess the capability of healthcare organisations to achieve cloud security and business missions. It seeks to define a progression that manages, measures, and controls all aspects of eHealth cloud security. To do so, it depends on five core indicators (IRM, IAM, ERM, PeS, PhS) for referencing and recognising security needs in a healthcare organisation.

It is very important for cybersecurity practitioners and executive decision makers to know their return on investment in security. It is even more essential to assess how suitable these investments are to safeguard their healthcare organisations as security policies, regulations, and threat settings are regularly changing (Beres *et al.*, 2009). These are the well-known vulnerabilities an organisation can experience.

The first stage of vulnerability is 'hardened', when the basic required security-related mechanisms, including patches, have been implemented. The next state is termed 'vulnerable', and it ensues when a minimum of one security update has not been implemented. The 'compromised' state occurs when the system has been successfully exploited (McHugh, Fithen and Arbaugh, 2000). For these vulnerability statuses, benchmarks are required to specify the organisation's security posture so that the period of susceptibility can be reduced by using a standard process to eradicate the susceptibility and its related threats. The degree of threats can be reduced if organisations are aware of their security posture. Therefore, the proposed model considers four levels of compliance.

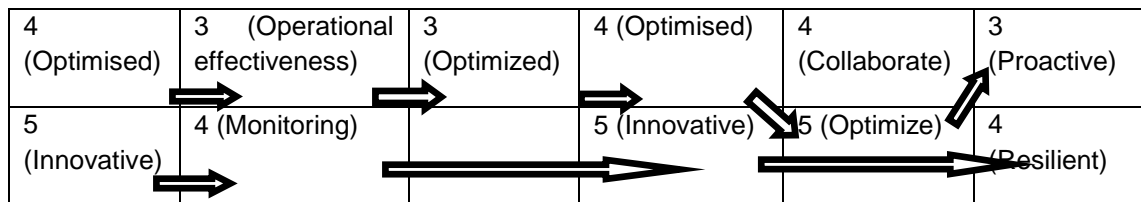
eHealth cloud security is assumed to progress as the healthcare organisation moves up these four levels (

**Figure 5.4).** A detailed description of the model in tabular form is attached in Appendix B.

The maturity levels of M<sup>2</sup>HCS are built upon the generic level indicators of the foundational maturity models. This is done because these maturity models make use of maturity levels that are either identical to or strongly resemble the capability maturity model (CMM), which is suggestive of the generic usefulness and validity of these levels. However, the maturity levels in the proposed model underwent minor changes (**Error! Reference source not found.**).

The maturity levels of M<sup>2</sup>HCS are defined from this viewpoint: A level zero (0), ‘undefined’, is contained within the model, similar to some CMMs. Level zero (0) contains objectives that imply that no capability whatsoever exists. Although level zero (0) objectives are included, the level itself is not included as a maturity level. In this way, the CMM practise is followed.

CMM	ISFAM	CSCMM	NHS NIMM	HIN CMM	M <sup>2</sup> HCS
		0 (Undefined)			
1 (Initial)	1 (Design)	1 (Initiated)	1 (Basic)	1 (Initial)	1 (Reactive)
2 (Controlled)	2 (Implementation)		2 (Controlled)	2 (Anticipate)	2 (Compliant)
3 (Standard)		2 (Managed)	3 (Standardised)	3 (Interoperate)	



**Table 5.3 Influences of Foundational Maturity Models and Development of Maturity Levels**

M<sup>2</sup>HCS consists of four maturity levels, progressing from reactive, to compliant, proactive, and resilient (**Error! Reference source not found.**). The maturity levels specify advancement of maturity. Hence, they apply to each domain.

Maturity Levels	Level Description	Summary of Domain Practises
1	Reactive	Controls are operated reactively
2	Compliant	Solely standards-compliant
3	Proactive	Implemented, structured practises
4	Resilient	Real-time security practises

**Table 5.4 Summary of M2HCS Maturity Levels and Practises**

A healthcare organisation may proceed through these maturity levels to achieve a highly secure cloud-based healthcare system. It is expected that as the maturity level rises, the model presents some processes and descriptions to aid in the progress.

Each maturity level has a predefined set of characteristics:

#### Level One, Reactive

This level is the starting point for the healthcare organisations actively using cloud. It is characterised by the organisation having elementary practical implementation in security systems, which is considered disordered, unreliable, and ad hoc, and it reactively responds to attacks, probably due to loss of

resources from the attacks. Such healthcare organisations have no defined policies or procedures to protect them. Their primary focusses are on the professional activities of the organization, and there is limited consideration for securing the organisation.

#### Level Two, Compliant

At this level, the healthcare organisation begins to guarantee that its security mechanisms provide stability. A healthcare organisation creates awareness of fundamental risk assessments, key applications, and network security, but its applications are mainly ad hoc. The focus is on the protection of essential systems, resulting in the perception that their systems are protected. The organisation has labour-intensive and reactive procedures to govern security incidents, but it is mainly in the stage of implementing cybersecurity processes.

#### Level Three, Proactive

At this level, there is central supervision of cloud security-related issues and policies related to the healthcare organisation. A healthcare organisation at this level has implemented enterprise-wide risk practises in the cloud and structured practises for information security risks. It is accountable for these responsibilities, and security policies and procedures are implemented with suitable mechanisms to support awareness and compliance. Access controls are binding and are thoroughly supervised to ensure strengthened social credential. Security processes are introduced, with the owner's responsibility stated. Such organisations have programmed mechanisms to govern the source and range of incidents. They are mainly in the stage of implementation and automation of

cybersecurity processes. The focus is on the professional activities, end users, and monitoring of security threats and all related mechanisms are tested and promptly implemented. They are mindful of their security needs, and they invest in systems that protect the organisation.

#### Level Four, Resilient

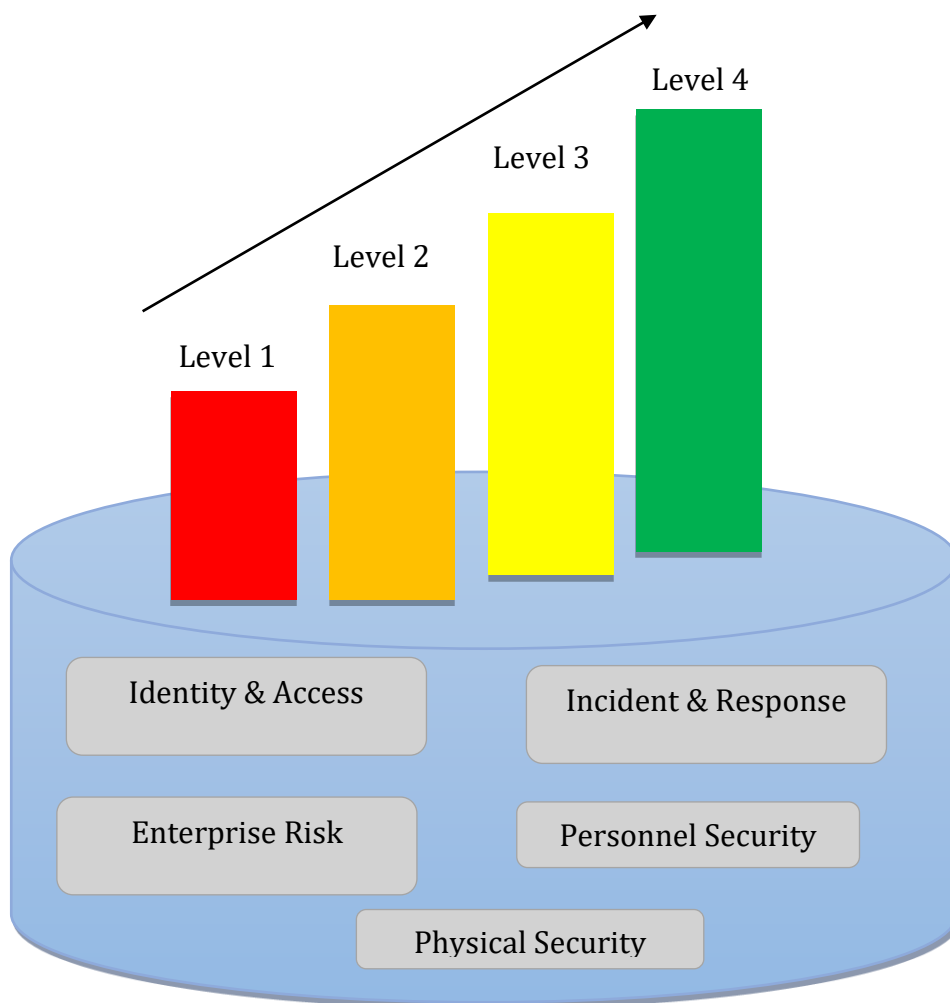
This level implies that an organisation is in control of its security needs. Such an organisation has real-time monitoring of risks and threats and uses risks assessment as a driver for security investment. At this level, there are proper policies and procedures implemented to prevent, detect, and correct eHealth cloud security-related issues. These are managed by identifying, reporting, and resolving security incidents, which ensures they are traced in an efficient way. The use of standard technologies throughout the healthcare organisation is a constant routine. Security of facilities ensures asset resilience and priority on physical security as well as cloud security. Resilient organisations are at the stage of sustaining and monitoring cybersecurity processes.



## Maturity Model for Healthcare Cloud Security (M<sup>2</sup>HCS)

Connected Medical Device, Physical Cloud Storage, Employee Awareness, External Personnel, Hospital Culture, Risk Identification, Risk Control and Monitoring, Risk Assessment and Response, Access Control, Lock out procedures, Mobile Device Management, Identity Federation and Provisioning, Firewall policies, Data Governance, Disaster Recovery, Incident Response and Handling Mechanism, Incident Reporting, Patch Management, Usability and Functionality

Objectives



Maturity Levels

Maturity Domains

**Figure 5.4 Detailed Dimensions of M2HCS**

### 5.3 Metrics

Metrics are measurement criteria that support decision making by assessing relevant data. A metric differs from a measurement, which calculates a single aspect of the object to be measured, whilst the metric is a result of two or more measurements to validate an essential association that can support decision making. Metrics are commonly multidimensional. They have lateral (administrative functions) and hierarchical (administrative levels) characteristics. To meet their projections, information system (IS) metrics should have these model features (Barabanov, Kowalski and Yngström, 2012).

- ⇒ Metrics must measure and express meaningful information (in content and presentation) in the proposed setting and to the target audience.
- ⇒ Metrics used should be easy to obtain; this ensures any flaws in data collection do not take all the resources required for successive steps of measurement.
- ⇒ Metrics should track targeted changes over an appropriate period.
- ⇒ Metrics must give specific and reliable numeric values using clear elements of measure.
- ⇒ Metrics must be constantly reproduced by different assessors under related settings; therefore, the measures must be well defined.

#### 5.3.1 M<sup>2</sup>HCS Metric

A design standard in existing maturity models is to demonstrate maturity as a number of levels, where the necessities of lower levels are accomplished to

progress to higher levels. Here, the principle is, in effect, 'what cannot be measured cannot be effectively managed'. A well-known example is the capability maturity model, founded on a strict design and stating a number of goals and/or key practises to achieve a predetermined level of complexity. However, the number of levels may differ based on the focus of the study; in the case of this research model, there are four levels.

Moreover, five domains have been developed to assess and manage the healthcare organisation's compliance with M<sup>2</sup>HCS. Each domain has its own core indicators, and these ten indicators are domain specific. They assess the security practises and the overall performance of the eHealth cloud. The assessment activities are intended as a guide to draw the assessors' attention to good practises and assist in evaluating the practises for their eHealth cloud.

For each control in a domain, a concise summary of practises mapped to the model's processes were described. The responses called for determine the level of operations in the healthcare organisation; however, some controls may not be applicable to the eHealth cloud and should, therefore, be ignored.

The level of operations is measured by allocating a four-point rating scale (based on maturity levels) to calculate how well the practises are performed. The domains require combined ratings of their predetermined activities to develop a comprehensive rating. An overall rating of all domains is made from an average of the domains, and this reveals the compliance with the proposed maturity model. The maturity level is then calculated using the M<sup>2</sup>HCS metrics flow chart, as shown in **Error! Reference source not found.** Maturity levels are assigned depending on the description of the

cybersecurity metrics. Afterwards, a maturity report is generated that describes all steps of the metrics and reveals the ultimate impact and consequences to the healthcare organisation.

#### 5.3.1.1 Decision Process for Assigning Maturity Level

The stages of the decision process are presented in the metrics flowchart depicted in **Error! Reference source not found.** Figure 5.5 and explained below.

Stage 1: The assessors obtain the healthcare organisation's business goals, including its related cybersecurity risks. Afterwards, tangible, written records and further spoken information are collected about the healthcare organisation's existing cybersecurity policies and activities. In this stage, the five domains and the four maturity levels used to assess these domains, and the electronic healthcare cloud security, are well defined.

Stage 2: The metric components and measuring methods are identified, along with the objectives for all domains. In this stage, the sub-dimensions (objectives) that are used to assess the domains for cloud security in the healthcare organisation are defined. Amongst the various objectives to be defined, the numbered ones in Figure 5.5 which are described as the core objectives, must be achieved in each domain.

Stage 3: Elements identified are surveyed and measured. To measure the electronic healthcare cloud security in the healthcare organisation, the objectives/control activities are measured and assessed based on the multiple statements of activities obtained from the healthcare organization.

Stage 4: Using the information collected in the second and third steps, each objective/control activity of electronic healthcare cloud security in the healthcare organisation is measured. Afterwards, a rating is created for the maturity level of each objectives/control activity and is assigned based on the organisation's particular statement(s) of activities.

Stage 5: The maturity level for each domain is calculated. Next, by calculating all the objectives/control activities of the domains, the maturity level for each domain is calculated based on the average of all the maturity rates for all objectives/control activities. Afterwards, the overall maturity level is calculated for all the domains in the proposed maturity model, M<sup>2</sup>HCS. The overall maturity level is the average of the maturity of all the domains. To calculate the overall maturity level using M<sup>2</sup>HCS, the formula in Equation 1 is used.

Stage 6: This stage checks for additional information obtained. If there is none, the process proceeds to the next step; otherwise, it returns to Stage 4.

Stage 7: A list of security practises to support the maturity progression of electronic cloud security in the healthcare organisation is proposed using the steps in section 5.3.2.

Stage 8: The progressive practises are put in place for implementation to produce improved security policies and processes in the healthcare organisation.

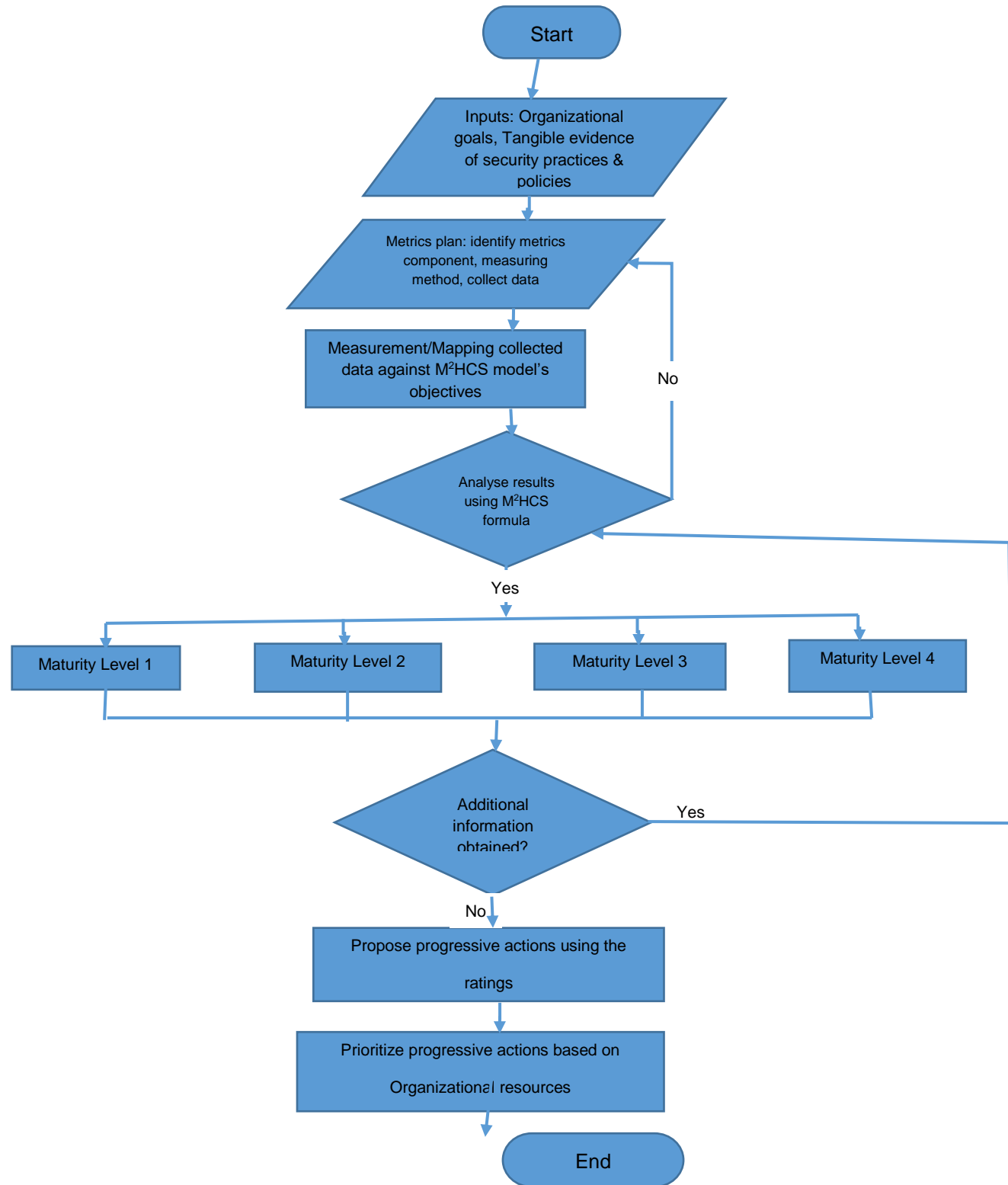


Figure 5.5 M2HCS Metrics Framework

### 5.3.1.2 How to Measure

Compliance to the model's features, listed previously, is usually necessary. However, in practise, many organisations may fail in their ability to do so (Jansen, 2009). The two most crucial concerns are as follow:

- ⇒ Qualitative IS measures are still the standard in most organisations which are not completely competent, resulting in decisions often based on individual information.
- ⇒ Quantitative IS measures are assessed without displaying connection with other elements, making their results not entirely beneficial for decision making (Axelrod, 2008).

It is important to understand which diverse measures can and cannot be used to specify required results (Herrmann, 2007; Jaquith, 2007; Axelrod, 2008). For instance, there is a major drawback in the use of the statistical forms of metrics in M<sup>2</sup>HCS. For example, calculating an average of the performance of a number of domains and controls may deliver a comprehensible and revealing measure of the overall security posture of healthcare organisation. However, it also conceals the fact that some domains and controls may be performing below the anticipated aim, whilst the average may be above it (Jaquith, 2007; Payne, 2007).



With reference to Stage 5, the final maturity level is calculated by this formula:

$$\beta = \sum_{d=1}^n (L_d) / n$$

**Equation 1 M2HCS Formula**

where  $\beta$  denotes final maturity level,  $\sum$  denotes summation of domain levels,  $d$  denotes domain,  $L$  denotes level for each domain, and  $n$  denotes number of domains.

### **5.3.2 Assessment Using Adopted Healthcare Domain-Specific Metrics**

Most of the existing cybersecurity assessment practises emphasise assessing cybersecurity programme efficiency (E Chew *et al.*, 2008) or measuring specific IS components like networks (Jansen and Grance, 2011). After making the choice of appropriate security metrics, a security metrics suite must be developed to deliver the healthcare organisation a means to achieve, manage, or develop the cybersecurity domains (Schimkowitsch, 2009). There is a fundamental requirement to outline security based on the needs of a specific organisation (Bishop, 2003). However, there is a similar understanding of what entails being secure or not. Consequently, broad established requirements and their corresponding key performance indicators can be expressed. This tactic has several advantages: It is easy to adopt the metric across diverse healthcare organisations to guarantee confident information sharing, and it influences cybersecurity validation enhancement.

To assess the maturity level of the M<sup>2</sup>HCS model, a domain-specific cybersecurity metric for healthcare organisations (Jafari *et al.*, 2010) was

adopted. The metric is domain-specific, but it is not custom made to a specific healthcare organisation's cybersecurity programme, which would enable peer implementation and appraisal of metrics results.

Cybersecurity metrics in this context possess three components: requirements, policy, and mechanisms (*CIS Security Metrics-Quick Start Guide v1.0.0*, 2010). Requirements describe security goals and objectives. Policy describes steps to reach these goals and objectives. Policy is derived from threat modelling, which can provide a variety of potential attack channels, some of which may be challenging to alleviate. Thus, other tactics like business continuity and recovery plans may be anticipated. Mechanisms put policy into effect and also refer to forms of protection (Schneier, 2004; 'Security for Cloud Computing Ten Steps to Ensure Success Version 2.0', 2015).

Elements of the metrics include technology maturity analysis, threat analysis and modelling, requirements establishment, policies and mechanisms, and system behaviour. Technology maturity analysis offers minimum and maximum sets of tools appropriate for the healthcare organisation. This will ensure uniform application of threat modelling, requirements, and comparable metrics results to monitor technology implementation. Threat analysis and modelling are contained in technology maturity analysis results. These are based on three assumptions: healthcare organisations strive to diminish attack surfaces; for each threat, there may be many ways to contain the situation; and healthcare organisations can select none, one, or more of the tactics to diminish the threat (E Chew *et al.*, 2008).

A generic set of requirements is formulated from threat analysis, regulations, and best practises. Each healthcare organisation devises its own policy and chooses a set of mechanisms to implement that policy. If the threat analysis assumptions are true, then the measurement process must entirely assess the policies and mechanisms to ensure comparable results. Lastly, information on incident tendencies and successful attacks are to be collected and analysed, and information related to operational behaviour must be monitored.

Table 5.**Error! Reference source not found.**5 (below) illustrates letting  $T$  be threat modelling results,  $R$  be a generic set of requirements, and  $S_p$  be a set of values depicting security posture of a measured healthcare organisation. Let  $P$  be a set of policy-describing requirements,  $R$ , and let  $M$  be a set of mechanisms for enforcing policy  $P$ . For a single set of requirements  $R$ , organisations may deduce several policies:  $P_i: i = 1, 2, p$ . For each policy  $P_i$ , several different mechanisms can be derived:  $M_j: j = 1, 2, m$ , where  $m \geq n$ . It is expected that, at minimum,  $S_p$  can reveal relatively comparable results if  $P$  and  $M$  are assessed entirely and  $R$  is made to fulfil  $T$ . Since security is a process (Schneier, 2004), it is important to include general performance indicators for  $P$  and  $M$ . Thus,  $S_p$  is not a single value but rather a set of values.

S <sub>P</sub>		Generic Requirements (R) ⇒ Derived from threat modelling (T)			
	P & M	Systems acquisition and configuration ⇒ Machine monitoring ⇒ Patch management ⇒ Systems upgrade, ...			
		Usage scenarios ⇒ Access control levels ⇒ Policy violations ⇒ Identification & authorization, ...			
		Incident reports ⇒ Number of blocked/unblocked attacks, ...			

**Table 5.5 Elements of Security Posture (Jafari et al., 2010)**

To avoid measurement distortion, the cybersecurity metric tries maintain these challenging characteristics (Herrmann, 2007; Jaquith, 2007):

- ⇒ Precision: the extent that repeatable, concise results can be demonstrated for several measurements taken under similar conditions
- ⇒ Accuracy: the degree of agreement of individual or average measurements with an accepted reference value or level
- ⇒ Validity: degree to which it measures what was intended to be measured
- ⇒ Correctness: the degree of formality adhered to during the measurement process
- ⇒ Cost effectiveness: that metrics data must be inexpensive to gather in terms of time and cost, and preferably gathered automatically

M<sup>2</sup>HCS is a model that healthcare organisations can use to secure these characteristics and cloud capabilities connected with their processes. As the healthcare organisation progresses from one maturity level to the next, the variety of benefits from improvement practises increases significantly. This is because progresses from each maturity level addresses various elements of security in eHealth cloud, and different remunerations occur at each level.

#### **5.4 Senior Management Support**

An important success factor for a good cybersecurity metric is the support and active involvement of executive management (Elizabeth Chew *et al.*, 2008). The lack of a good model for mapping IS metrics to the specified setting, and plainly explaining the quantitative measures, results in security assessors frequently struggling to find a concession between reporting metrics that are too technical for the senior management and ones that damage the use of a metric due to generalisation (Mimoso, 2009). The M<sup>2</sup>HCS model and its metrics present a qualitative and quantitative assessment of the cloud security of the healthcare organisation. For executives, it provides a detailed security assessment of the eHealth cloud to aid in decision making. For security experts, its quantitative metrics support proactive and reactive processes.

#### **5.5 Chapter Conclusion**

This chapter discusses the development methodology process of the M<sup>2</sup>HCS model and metrics. Further descriptions of the model in this chapter include a logical approach that includes a detailed method for assessment (model matrix/table), a metrics framework, and an adopted healthcare-domain-specific

metric tool. The model includes relevant aspects of healthcare cloud security and plainly describes what individual levels mean for each control. Its descriptions are focussed on practises. Individual control is measured as a capability maturity, letting a healthcare organisation measure where they are with respect to a particular security control and to assess improvement over time or against a goal, even if it is ongoing. The security model matrix/table can also be used as a list of commendations to detail how the healthcare organisation may attain its cloud security objectives. Each domain, with its set of controls for each maturity level, is clearly defined. Lastly, M<sup>2</sup>HCS can be used for observing intra-organisational cloud security over time, measuring progress made by the organisation's policies, and attaining a goal recognised through study of similar healthcare organisations' cloud security proficiencies.

The following chapter discusses the validation of the proposed model by IT healthcare experts, which, in turn, informs the formulation of a prototype system that encompasses the key functionality of M<sup>2</sup>HCS.

## Chapter Six

### 6 Validation of Maturity Model for Healthcare Cloud Security

This chapter describes the validation step of Design Science Research Methodology, which considers the validation process one of the most central aspects of research. This ensures the development of a solution step because it is the validation process that authenticates the contribution of the solution, along with its usefulness, value, and ability in regard to the acknowledged problem (Hevner *et al.*, 2004).

#### 6.1 Validation Strategy

The validation strategy of the proposed model, Maturity Model for Healthcare Cloud Security (M<sup>2</sup>HCS), and its metrics was carried out by means of:

1. A case study
2. Survey/interviews with practitioners
3. Feedback from the scientific community through the submission and presentation of academic papers

Results ascertained that M<sup>2</sup>HCS offers a suitable and strong progression method and is dependable when it comes to improving functioning healthcare cloud security services. These validation methods are further explained below:

- ⇒ Case study: A fabricated scenario to prove the model and its use to resolve the research problem. Its objectives include validating the proposed controls and domains by adding or removing them from the model matrix, which is expected to make advances to the model, and collect information related to the processes used to manage security services in the eHealth

cloud to perform the assessments. M<sup>2</sup>HCS was applied to an NHS Trust University Teaching Hospital, from which a case study was fabricated.

- ⇒ Survey and interview: Collected feedback through survey and interviews with practitioners regarding the model, capacity to follow its stages, and potential to achieve appropriate results. Its objectives are the same as the case study's (above). Furthermore, the execution of the online survey and its applicability were discussed. Six of the experts involved in the survey were asked further questions in interviews.
- ⇒ Scientific publications: Submit research papers to obtain a review from the scientific community.

This validation method follows the design validation guideline within DSRM (Hevner *et al.*, 2004). In conclusion, after the completion of the steps in this validation process, adequate information can be collected to resolve the uncertainty of returning to modify the prior objectives/controls defined for the model or perform amendments to the proposed metrics, continue onward, and communicate the results of this research.

## **6.2 Survey and Interview**

This section discusses the means through which the survey and interviews were piloted and presents the results gathered in the course of that procedure. To assess the proposed and crucial objectives/control activities, the researcher established six surveys and conducted semi-structured interviews with relevant experts. The opinions of the expert participants were particularly useful because they included both clients and suppliers. The suppliers interact with a wide range



of clients and, thus, have knowledge about what the clients must do to secure and manage their services in the eHealth cloud. The clients are the real end users of the models, so they provided information based on the present security needs in their healthcare organisations.

The purpose of these surveys and ensuing interviews was to enquire, of individuals with expertise regarding the application and optimisation of electronic healthcare cloud security services, whether or not the M<sup>2</sup>HCS is viable and valid.

**Error! Reference source not found.** provides information about the expertise and roles of the survey participants. Their roles and locations are listed in the first column. In the second column, the expertise of each participant is given to define the reason he or she was suited to offer an expert view. **Error! Reference source not found.** also presents the scales of measurement for the survey.

#### 6.2.1 Background of Study Participants

The study participants were identified through a web search of the appropriate persons with roles in security assessment and management in eHealth cloud, health IT departments, research contributions in health informatics, and the field as a whole. An e-mail consisting of a letter of introduction and purpose of the survey was sent to the seventy individuals selected for participation; six people responded. These six experts agreed to partake in the survey. However, three who contributed to the survey declined to partake in subsequent interviews as they were not available. Table 6.1 presents the pre-assessment information about the participants of the survey. Their contributions in forms of survey and interview responses formed the basis for these findings.

Position	Participant Code	Background	Years	Healthcare Facility	Experience Assessing	Type of Assessment
CIO	PR	Medical informatics	30	University Hospital	Yes	Internal/External
CIO	NO	Medical informatics	17	Acute Academic Hospital	Yes	Internal/External
Researcher	LBS	Medical informatics	10	Medical Research Industry	Yes	Internal
Professor	WH	Medical informatics	15	Academia	Yes	External
COO	DOB	Cybersecurity	12	Cybersecurity Industry	Yes	External
Director	BK	eHealth security	16	Medical Device Manufacturer	Yes	Internal/External

**Table 6.1 Pre-Assessment Information about the Participants**

The interviews consisted of online meetings (making use of Skype) and the survey questionnaire. At the beginning of the Skype meeting, the researcher presented the objectives of the survey questionnaire and a brief justification of the need for the ensuing interview. During the survey, the participants were asked to evaluate the set of domains and key controls/objective activities in the maturity model M<sup>2</sup>HCS, using the scale presented. The participants were also asked to further expound on their survey responses and propose modifications or add-ons to the existing set of domains and key controls/objective practises to better adapt them for the eHealth cloud security maturity assessment. The following sections present the results from the surveys and interviews (Section 6.2.3) and the influence of this feedback on the proposed model (Section 6.2.4).

Given the detailed scope of the research, it was very important to speak to relevant experts in the field who would offer informed assessments on the challenges of eHealth cloud security practises in hospitals (Table 6.2). With the limited number of participants, the use of additional interviews was considered.

However, given the schedules and availability of the participants, conducting the interviews would have required more time beyond the submission of this thesis.

For reporting purposes, and to protect participants' identities, each participant was assigned a pseudonym to ensure their anonymity. Participants of the survey study were assigned the codes PR, WH, LBS, BK, DOB, and NO, respectively. At the time of the study, the participants contributed differing amounts of information about the domains' key activities. Some talked at length about one domain, whilst others made nearly equal contributions across all five domains. However, it was ensured that all participants' voices and views are represented in this study.

Roles (Location)	Expertise
Chief Information Officer (Australia)	He has over 30 years' experience as an expert in implementation of clinical systems in large healthcare organisations and the management of health information systems, including senior ICT management roles as CIO in a university hospital and as IT manager of hospitals. He has performed in consulting roles, including a validation of and report on global best practises for digitised healthcare decision support. He has broad experience in managing telehealth initiatives, including the Telehealth Pilot Programme and Primary Health Network on Information Systems Strategy and Cybersecurity.
Chief Information Officer (Europe)	A director of informatics in the largest acute academic hospital with corporate responsibility for information communication technology (ICT), He acted on the National Integrated Medical Imaging System (one of the largest single PACS/RIS solution implementations in the world) Project for the Health Services Executive. In addition to his academic appointments, research interests in health informatics, several peer-reviewed publications and presentations at conferences, he is a recent chair of a health informatics society.
Researcher (Europe)	He currently works at a company that provides computational solutions for better decision making and knowledge management in health care industry. He has been involved in European projects, such as MedBioinformatics H2020, European Medical Information Framework Platform (IMI), and EU-ADR. As a researcher, he has worked on projects related to sharing more than 30 million medical images in distributed environments and cloud computing. He has specialities in large-scale storage and databases (cloud computing such as AWS, Azure, Google AppENGINE, RackSpace), medical networks, and medical imaging experience (healthcare sector).
Professor (USA)	He is a professor in the department of radiological sciences and a member of a medical imaging and informatics group. His research specialities include predictive modelling, population health management, and imaging informatics. He is an active member of the American Medical Informatics Association and a leader in the Imaging Informatics Working Group.
Chief Operating Officer (Asia)	He has specialities in ensuring effective and engaging security awareness programmes, critical infrastructure protection, information governance, risk, compliance, security audit, ethical hacking, incident management, ISMS, BCP/DR, standards, frameworks, readiness/implementation/audit, and metrics.
Director (Europe)	An experienced security and privacy officer working for a large global organization developing medical products and services. Currently working on defining corporate policies and requirements, processes, regulations, and standards, performing privacy and security impact assessments, event management, auditing, and developing common tools and technologies. This programme ensures that they are implemented to safeguard medical devices and services that are in compliance with legislative and healthcare requirements and resilient against cyberattacks.

**Table 6.2 Summary of the Research Participants**

### 6.2.2 Survey and Interview Protocol

- ⇒ The researcher explained what the research is about in an electronic e-mail and 'Information' document. The participants' consent was read and signed by clicking the 'Agree' button in the 'Questionnaire' document (refer to Appendix C for a sample of this document).
- ⇒ A few pre-assessment (stated as 'Respondent Details') questions (Table 6.1) **Error! Reference source not found.**were asked in the 'Questionnaire' document. They are as follow:
- What best describes your current position?
  - What is your background: academia, healthcare, cloud security, cybersecurity?
  - How many years of experience do you have in this field?
  - Do you have any experience in healthcare cloud/cybersecurity? If so, how many years?
  - What was the type of healthcare facility: general/acute-care hospital, community health centre, district hospital, specialised hospital, teaching hospital, clinics, private healthcare centre?
  - Have you participated previously in cloud/cybersecurity maturity assessment? Type of assessment?: yes, no, internal (within an organisation), external (outside an organisation)
- ⇒ The conceptual framework established in section 5.2 was used to give details about the elementary subcomponents of the model M<sup>2</sup>HCS.

- ⇒ The conceptual framework was used to describe and assess the appropriateness of the proposed model. The researcher made this process easier by providing detailed information about the elementary subcomponents of M<sup>2</sup>HCS. By doing this, the survey participants were acquainted with the comprehensive information about the domains, maturity levels, and objectives of the proposed model.
- ⇒ The interview participants provide answers to the assessment questions.
- ⇒ The survey questionnaire utilised the Likert scale (**Error! Reference source not found.**) and 'Further information' question types. A question was asked, for which the scale provides four possible responses:
  - Strongly Disagree
  - Disagree
  - Agree
  - Strongly Agree

The Likert scale supports the researcher by providing possible answers ranging from 4 (strongly agree) to 1 (strongly disagree) to indicate whether the survey participants agreed or disagreed with each question to measure the 'Further information' provided on a certain statement. The Likert scale was also chosen because it is a familiar interface used in many surveys. The conversant structure allows the survey participants to better comprehend and respond to the questions.

Strongly Agree
Agree

Disagree
Strongly Disagree

**Table 6.3 Scale Used in the Survey**

### 6.2.3 Survey and Interview Results

This section presents the data collected during the design and development step of DSRM. The key objective was to validate the domains and objectives/control activities used in the proposed model, M<sup>2</sup>HCS, and to better adapt it to the electronic healthcare cloud through the deletion, addition, or modification of these domains and practises. The outcomes of the survey are shown in the following section.

#### 6.2.3.1 Maturity Model Validation Feedback

To satisfy the model's operational characteristics (OC), the researcher provided data about how the proposed maturity model, M<sup>2</sup>HCS, is presently effective regarding applicability to electronic healthcare cloud security assessment (OC1). Therefore, the researcher has included the questions below to achieve that (at the beginning of the assessment in **Error! Reference source not found.**). The feedback revealed that the majority of the participants agreed (chose 'Agree') with the maturity model validating questions, with an overall mean of 2.88.

Questions	Mean of Feedbacks
Are the domains relevant for the assessment of maturity within a healthcare organisation?	3.0
Are the objectives relevant?	3.0
How feasible would it be to assess these objectives in practise?	3.0
Can the maturity model be practically used in the healthcare industry?	2.5
Overall mean: $3.0 + 3.0 + 3.0 + 2.5 =$	2.88

**Table 6.4 Maturity Model Validation Feedback**

There was strong agreement amongst survey participants concerning many of the survey questions. After the pre-assessment questions, questions were asked to validate the overall model. The researcher established from all the responses of the survey participants that the domains are relevant for the assessment of maturity within a healthcare organisation (OC4). All the survey participants chose the 'Agree' option; however, some made recommendations to better adapt the relevance of domains for the assessment of maturity within the context:

*Agree, but would recommend to call out at least supplier management and acquisition as a separate domain or include it as an item in all domains as there are requirements for that in each of them as they are now somewhat hidden in the domains.*

Furthermore, the survey participants chose the 'Agree' option as to the relevancy of the objectives/activities (OC3):

*Agree, but need a clear distinction between the objectives of the organization and how to achieve them as for cloud some are internal, some are external (which means internal needs to spec and check).*

Thirdly, all survey participants chose the 'Agree' option for the feasibility of assessing these objectives/activities in practise (OC4):

*Agree in that it would be feasible to assess the objectives, although some need better descriptions as they are not clearly stated as an objective.*

The last question assessed the validation of the overall model by determining its practicality in the healthcare industry (OC1):



*Agree mostly because of the setup but disagree mainly because of the structure. Healthcare providers are being pushed by regulations (e.g. GDPR and NIS) towards appropriate security and privacy management. Often this is done towards established security frameworks like ISO 27001. As there are already recognized standards in the area of cloud computing (ISO/IEC 27017) and health IT (ISO/IEC 27799), I would like to recommend something that could be mapped against the high-level structure and these ISO standards.*

#### **6.2.3.2 Domain, Maturity Levels, Objectives Validation Feedback**

In the next section, questions were asked to validate the operational characteristics of the objectives/activities. The four questions were answered with varying opinions from survey participants. Further discussions of these outcomes are given below.

From the first question, the researcher established from all the responses of the survey participants that each domain's objectives/activities were correctly assigned to maturity levels for the proper assessment of maturity within a healthcare organisation. All the survey participants chose the 'Agree' option.

The other questions about each domain's objectives defining progression across maturity levels, modification/realignment of each domain's objectives, and research designated choice of each domain's core objectives resulted in varying outcomes (outlined in **Error! Reference source not found.**). The domain, maturity levels, objectives, and validation feedback (**Error! Reference source not found.**) revealed that the majority of the participants chose between a variance

of 'Agree' and 'Disagree' for the maturity model validating questions, with an overall mean of 2.43.

Questions	Mean of Feedback
Do you consider the descriptions correctly assigned to their respective maturity levels?	3.0
Do you consider the controls appropriate for defining levels?	2.0
Do you consider the core control descriptions appropriate to maintain a maturity level?	2.3
Overall mean: $3.0 + 2.0 + 2.3 =$	2.43

**Table 6.5 Domain/Maturity Levels/Objectives Validation Feedback**

Questions	IAM	IRM	ERM	PeS	PhS
Do you consider each domain's objectives/activities correctly assigned to their respective maturity level?	Agree	Agree	Agree	Agree	Agree
Do you consider each domain's objectives/activities appropriate for defining maturity levels?	Disagree	Agree	Disagree	Agree	Disagree
Do you consider each domain's core objectives/activities appropriate to attain the maturity level?	Disagree	Agree	Agree	Agree	Agree
Which of each domain's objectives/activities would you add or remove?	Data governance should be in ERM, while handling data breaches	Add emergency access policies and procedures	Data and security governance and overall security risk management	External personal security could be misread as contractors. Move suppliers	Add connected medical devices into physical security rather under ERM. If only talking

	should be in IRM. Disaster recovery should be treated as a separate domain.		should be added	to a separate domain for clarity.	about segmentation, then it could remain.
--	---	--	--------------------	---	--

**Table 6.6 Survey Outcomes from Participants on Domains**

#### 6.2.4 Influence of Feedback on Proposed Maturity Model

In this segment, the researcher utilised the survey participants' feedback (presented earlier) and performed an analysis on it to gain realistic knowledge for the construction of the proposed maturity model for healthcare cloud security.

The Likert scale ratings (**Error! Reference source not found.**) were used to assess the survey participants' validation feedback (section 6.2.3.1). The Likert scale rated the response to each question and the overall mean to find the survey participants' overall feedback for each validation question during the analysis.

**Error! Reference source not found.** shows the survey feedback to validate the proposed maturity model. All of the six survey participants provided feedback on the applicability and effectiveness of M<sup>2</sup>HCS in the assessment of security practises in a healthcare organisation actively using the electronic healthcare cloud. The rate of recurrence in the feedback revealed that most of the survey participants chose 'Agree' in response to most of the questions.

Regarding the validation of the domain, maturity levels, and objectives, the survey feedback revealed that most of the participants chose the 'Agree' option to show that all the given aspects are essential to support significant activities in the framework of the proposed maturity model (OC4). The survey participants' also confirmed the significance of each aspect's constituents. The averages displayed

that the survey participants were in agreement with the questions, though some gave recommendations to add new, or remove or reshuffle, objectives. Four survey participants provided feedback to approve this requirement. The others emphasised the need to think through the skills and awareness of the security assessors involved in the healthcare organisation. Despite this, they all agreed by stating that from their assessment of M<sup>2</sup>HCS, it provides a guide using a well-thought-out and methodical approach to the optimisation of security practises of electronic healthcare cloud (OC1).

Furthermore, the survey participants also validated the proposed maturity model's usability in relation to simplicity, clarity, practicality, elasticity, and competence (OC2). All six survey participants' feedback established that the proposed maturity model and metrics are easy and natural to follow.

Regarding the rationale for their views, the participants provided some comments to support their opinions, as follow:

- ⇒ All six survey participants' feedback also acknowledged that executive decision makers could obtain their informed decisions from the assessment results and format (OC5).
- ⇒ It was mentioned that there should be a separate domain for supplier management or to include it as an objective/activity in all domains.
- ⇒ A need for clear distinctions between the objectives of the organisation and how to achieve them (OC3) were mentioned. As for cloud, some are internal and some external.

⇒ Lastly, all six survey participants' feedback further established that the proposed model, M<sup>2</sup>HCS, is not directly drawn from any other standards, technologies, or concrete implementation details. However, there were recommendations that M<sup>2</sup>HCS could be further mapped against related regulations because healthcare organisations are being pushed by regulations towards appropriate security and privacy management.

### **6.3 Proposed Maturity Model Changes and Improvements**

For qualitative feedback, the validation of the framework of the maturity model contained open-ended statements to give participants an opportunity to express further comments and recommendations about how to update and improve the proposed model. The qualitative feedback contained the suggestions below:

- ⇒ Overall Maturity Model: Healthcare providers are being pushed by regulations (e.g. General Data Protection Regulation) towards appropriate security and privacy management. It was recommended that the proposed maturity model should be mapped to established security frameworks like Information Standards Organization (ISO) 27001, ISO 27017, ISO 27799, ISO 80001, and ISO 27005.
- ⇒ Incident & Response Management Domain: It was mentioned that some objectives/control activities were too prescriptive, making the subject fail to comply with the Incident response management requirements. The objectives/activities were refined to be clearly distinct and descriptive about how to achieve them.

- ⇒ Identity Access Management Domain: Again, it was mentioned that some objectives/control activities were too prescriptive. The objectives/activities were refined to be clearly distinct and descriptive about how to achieve them.
- ⇒ Enterprise Risk Management Domain: All of the validation survey participants suggested relocation of data governance to this domain and stated that security governance should be added in this domain.
- ⇒ Personnel Security Domain: Most of the validation survey participants referred to the fact that 'external personnel security' should be rephrased to properly suit contractors. Third parties' security (the rephrasing of 'external personnel security') contained details about supplier management, as recommended in the feedback.
- ⇒ Physical Security Domain: Some of the validation survey participants commented that connected medical devices should not be included in physical security but rather under ERM, except if it is only focussed on segmentation, which in this case it was.

The survey participants made the recommendations that needed to be addressed in the refinement of the proposed framework of M<sup>2</sup>HCS; these suggestions are reviewed in section 6.3.16.2.3.1 below.

### **6.3.1 Framework Refinement**

The validation process was designed to test whether the proposed framework could be used in the practical context of assessing security practises within

healthcare organisations actively using cloud by adding, removing, or modifying components, as shown in Figure 5.4.

The recognised objectives for the proposed maturity model were validated through the survey, and the outcomes of the study are shown in **Error! Reference source not found..**

As discussed, the survey participants recommended refining the framework of the proposed M<sup>2</sup>HCS. Therefore, their recommendations were deliberated on and put into this research to improve the framework of the proposed maturity model. These recommendations were painstakingly thought out, and the framework of the model was revised in this way:

- ⇒ Maturity Model: It was mapped to present high-level compliance to earlier recommended standards. This is because healthcare providers are being pushed by regulations towards appropriate security and privacy management. The recommended standards, ISO/IEC 27017 and ISO/IEC 27799, are considered established security frameworks that are complied with by healthcare organisations using cloud deployments (OC1).
- ⇒ IRM Domain: Its objectives were thoroughly reviewed, and prescriptive descriptions were turned into high-level descriptions to allow flexibility when making the choice of solutions to be implemented. The objectives were refined to be clearly distinct and descriptive about how to achieve them (OC3).
- ⇒ IAM Domain: Its objectives were thoroughly reviewed, and prescriptive descriptions were turned into high-level descriptions to allow flexibility when making the choice of solutions to be implemented. The

objectives/activities were refined to be clearly distinct and descriptive about how to achieve them (OC3).

⇒ ERM Domain: Data governance was transferred to this domain and renamed 'information assurance'. This choice was made to cover both data governance and clinical/corporate governance.

⇒ PeS Domain: External personnel security was changed to 'third parties' security'. This objective would encapsulate the contractors, external personnel, and suppliers.

⇒ PhS Domain: Connected medical devices remained in this physical security domain. This was because its activities were mainly focussed on segmentation only.

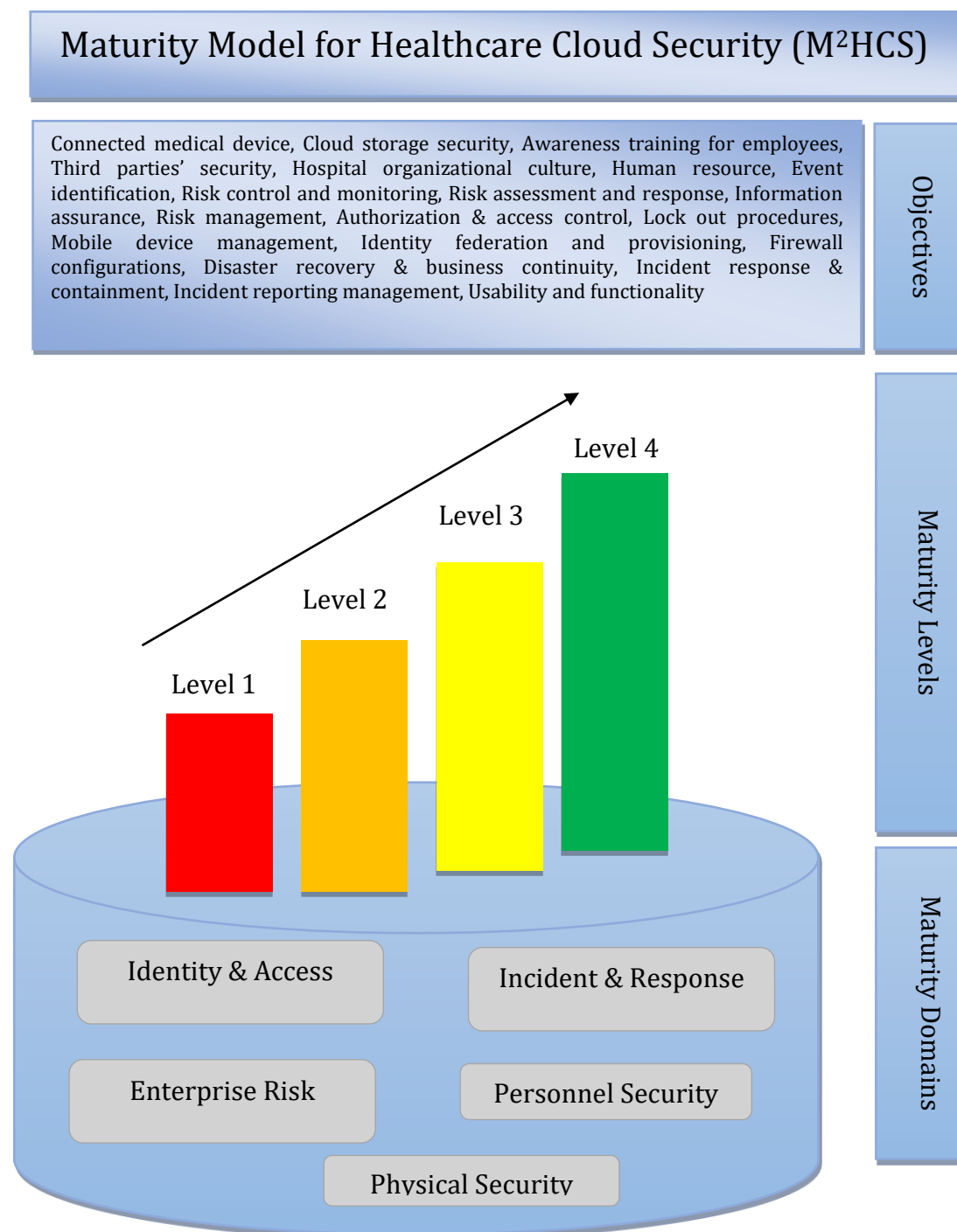
Domains	Objectives/Controls	Refinement Recommendations
IRM (Incident Response & Management)	Firewall configurations	
	Data governance	Transferred to ERM domain
	Disaster recovery (DR)	DR/business continuity
	Incident response (IR)	IR & containment
	Patch management	
	Incident report management	
		Incident preparation
		Incident detection & analysis
IAM (Identity & Access Management)	Authorization & access control	
	Log off of system users	Safety regarding lockout
	Mobile device management	
	Identity federation & provisioning	
ERM (Enterprise Resource Management)	Data governance	Information assurance
	Event identification	
	Risk control & monitoring	
	Risk assessment & response	
PeS (Personnel Security)	External personnel security	Third parties' security
	Awareness training	



	Hospital organisation culture	
		Human resources
PhS (Physical Security)	Cloud storage	Cloud storage security
	Connected medical device	

**Table 6.7 Refinement of M2HCS framework**

The revised scheme of the proposed maturity model to assess, maintain, and improve a healthcare organisation's effective cloud security practises is presented below in Figure 6.1.



## **Figure 6.1 Revised M2HCS**

### **6.4 Practical Validation of the Research Findings**

In addition to the previous validation approach, the researcher decided to further assess the proposed maturity model in a real-case scenario. Therefore, a single case scenario was developed and used to further examine the practicality of using the proposed model for healthcare cloud security in an everyday healthcare organisation actively employing cloud services. The case scenario considered an NHS Trust University Teaching Hospital in the United Kingdom, which was implementing some cloud computing services. To do this, their security practises were obtained from their web-based published policy documents. Afterwards, an instrument was designed and developed that assisted the decision maker (researcher) in assessing the identified cloud security practises of this hospital based on M<sup>2</sup>HCS. Lastly, the identified security practises were improved by implementing the recommendations obtained from the use of the healthcare-domain-specific metrics/framework.

This proposed maturity model was designed and developed for analysis purposes. Nevertheless, its potential is extensive, and it can be used to:

- ⇒ support decision makers in their assessment of security practises in healthcare organisations actively using cloud services

- ⇒ enlighten decision makers about the existing maturity levels of security practises in their healthcare organisations actively using cloud services
- ⇒ educate decision makers about their healthcare organisation's weak and strong security practises within each domain of the proposed maturity model
- ⇒ provide recommendations for decision makers to improve their healthcare organisation's weak security practises in cloud services implementation based on their identified maturity rating
- ⇒ prioritise the provided recommendations based on available resources within the healthcare organisation

Thus, M<sup>2</sup>HCS is metrics framework useful in the decision process for assigning maturity levels.

#### **6.4.1 Demonstration of Case Study Stage**

This section relates to the demonstration step of DSRM. To demonstrate the model M<sup>2</sup>HCS, it was applied it to some security practises of an NHS Trust University Teaching Hospital in the United Kingdom. For this case study demonstration, efforts were made to present an all-inclusive description of the specified security practises of the model. In section 6.4.3, the case-study hospital's cloud security assessment and summary are discussed, and a proposal for the improvement of its cloud security practises is based on obtained results and main conclusions.

This case study was chosen because the healthcare organisation was considered a representative of the average NHS Trust University Teaching

Hospital. The study seeks to measure the applicability of M<sup>2</sup>HCS to a real healthcare organisation. It was expected that it could provide ways to improve their maturity levels as this would also improve its security practises and processes and, in effect, its healthcare delivery. To conduct these demonstrations, the model was applied to specified practises of the hospital (which has more than 100,000 admissions per year).

The researcher obtained information from the healthcare organisation's website and conducted a review of their current policies guiding their current security practises to formulate a case study. The case study describes the application of the model, emphasising physical security, personnel security, risk management, network infrastructure security, medical devices use and management, information security, information governance, incident management, and data protection practises and how they are being applied in the hospital. Finally, the model's metrics were applied to assess these practises and propose improvements.

#### **6.4.2 Case Study**

The initial phase was to report the activities implemented by the case-study hospital, based on policy documents. From this, the researcher presented a manuscript together with the application of the security practises. Following that, the researcher made a distinction amongst the security practises and processes according to the maturity model's domains, such as physical security, personnel security, enterprise risk management, incident response management, and identity, and access management. To achieve that, the researcher emphasised

the manuscript using **bold**, and *italics* to discuss the identified domains and practises, respectively. The researcher also used underline and brackets ( ) to identify the objectives.

The case-study hospital must continue making improvement in delivering the action plan to further develop its security practises and processes and meet requirements of the European Union General Data Protection Regulation (GDPR), amongst other key legislations and standards for maintaining security in healthcare. From the policy documents, the following information was extracted and arranged in appropriate paragraphs based on the domains for the purpose of building a case study (Scott and Harder, 2017). The following paragraphs are directly quoted.

#### **[Incident Response Management]**

*Suppliers are required to maintain and comply with a plan for business continuity and disaster recovery (incident reporting management) {4} for each of the goods and services it provides to the Trust, in order to mitigate, as far as reasonably possible, the impact of events or circumstances which could detrimentally affect the uninterrupted supply of the goods or provision of the services. *Reviews the existence and effectiveness of the policy, systems and procedures (incident response and containment) {4} in place Trust-wide in respect of major incidents and business continuity arrangements to ensure that they are in line with current legislation. Where cost effective and appropriate, resilience are built in to the infrastructure to mitigate the failure of any one component. All connections to external networks are firewalled (firewall configurations) {2} and where necessary**

include additional intrusion prevention measures. *Incidents and faults with the network are recorded (incident reporting management) {3}* within the Information Management & Technology business management system and the Information Management & Technology Service Desk (Scott and Harder, 2017). *Incidents will be reported (incident reporting management) {3}* on the Trust risk management system, and investigated accordingly.

### **[Identity and Access Management]**

Where supported, *network infrastructure device configurations are automatically collected and archived (mobile device management) {4}* by a central management system. There is a *documented and formal user registration and de-registration process for access to the network (authorization and access control) {3}*, held by the hospital's Information Management & Technology Service. *Security privileges to the network are allocated on the requirements of the user's job (authorization and access control) {3}*, rather than on a status or any other basis and this is configured within Active Directory or individual systems. *User access rights are removed or reviewed for those users who have left the Trust or changed jobs (authorization and access control) {3}* and user accounts are disabled automatically if not used in 100 days and deleted after a further 61 days. *Only equipment approved by the Hospitals IM&T Service is permitted to connect to the network and all equipment is registered (mobile device management) {3}* with the ICT Configuration Management Database (CMDB) (Scott and Harder, 2017).

## **[Enterprise Risk Management]**

The Hospital's Information Management & Technology Service *carries out security risk assessment(s) that covers all the aspects of the network (risk management) {2}* in relation to supporting all the business processes. The *risk assessment also detects all the applicable, cost-effective security countermeasures necessary (event identification) {2}* to protect against possible breaches in confidentiality, integrity and availability. Risk management is covered within the CCA 2004 and is the first step in the emergency planning and business continuity process. It ensures that local responders make plans that are sound and proportionate to risks. *Risk assessments can be undertaken through a specific planned process (risk assessment and response) {3}* at Corporate, Care Group or Service Line level. A risk should be recorded to Datix and for each *risk that cannot be resolved immediately an action plan to eliminate, minimise or accept the risk (risk assessment and response) {4}* is required. The actions must be recorded on Datix together with the risk grading following completion of the action plan. *Risks must be monitored at the appropriate level (risk control and monitoring) {3}* in accordance with the review, approval and escalation process (Scott and Harder, 2017).

## **[Physical Security]**

Network computer equipment is housed in a secure environment. *Entry to secure areas housing critical or sensitive network equipment is restricted (cloud storage security) {2}* to those whose job requires it. *Critical or sensitive network equipment*

*is housed in an environment that is monitored for temperature and power supply (cloud storage security) {2} quality. Critical or sensitive network equipment is housed in secure areas, protected by a secure perimeter with appropriate security barriers and entry controls (cloud storage security) {2}. The most effective method of controlling access is to restrict the number of Authorisers. Ideally, there will be one Door Access Card Authoriser per speciality/department (cloud storage security) {2} (Scott and Harder, 2017).*

### **[Personnel Security]**

The healthcare organization ensures *sufficient staff are aware and trained in the requirements detailed in relevant emergency response plans (awareness and training) {3}*—including business continuity arrangements, Major Incident Plan and relevant emergency response plans. *Third party access to the network is restricted only to those devices or systems deemed necessary and appropriate (third parties' security) {4} and all such access to the network is logged for audit (third parties' security) {3} purposes.* The Human Resources and Organisational Development Directorate is responsible for managing the process of *induction for new staff and delivery of Mandatory Training to all staff (awareness and training) {3}*. Ensures that new temporary and agency staff are provided with a Local Induction. Ensures that staff transferring from other locations within the Trust are provided with relevant elements of the Local Induction, and that this is recorded on the Local Induction checklist. *Ensure staff complete Mandatory and Update Training (awareness and training) {3}*, through review of reports provided by the



Workforce Development Team and detailed review of the Workforce Development drive (Scott and Harder, 2017).

### 6.4.3 Case Study Assessment

The stages of the decision process measures are presented in the assessment and analysis explained below (OC2).

Stage 1: The assessor (researcher) obtained the healthcare organisation's web-based published business strategic direction and its related key risks, according to different practises, in a document called 'Board Assurance Framework (BAF)'. It is the key strategic tool for the management of risks and assurance. In addition, written records of information were collected about the healthcare organisation's existing cybersecurity policies and activities. In this stage, the five domains and the four maturity levels were used to assess these domains and assess the electronic healthcare cloud security practises in the healthcare organisation (OC4).

Stage 2: The objectives for all domains were identified (OC3). In this stage, the sub-dimensions (objectives) used to assess the domains for electronic healthcare cloud security in the healthcare organisation were defined. In this case study, the researcher emphasised the manuscript using **bold**, and *italics* were used to discuss the identified domains and practises, respectively. Each practise mapped against the maturity model's matrix supported the identification of the objectives. The researcher emphasised the manuscript using underline and brackets () to identify the objectives.

Stage 3: Elements identified were surveyed and measured. To measure the electronic healthcare cloud security in the healthcare organisation, the objectives are measured and assessed based on the multiple statements of activities.

However, in this case study, there were no multiple statements of activities since it was drawn from policy documents by a single assessor.

Stage 4: Using the information collected in the second and third steps, the rating was created for the maturity level of each objective. After measuring each objective of electronic healthcare cloud security in the healthcare organisation, the maturity level for each objective was assigned based on its particular statement(s) of activities. The researcher emphasised the manuscript using brackets {} to identify the ratings of identified objectives.

Stage 5: The maturity level for each domain was calculated. After calculating all the objectives of the domains, the maturity level for each domain was calculated (OC1) based on the average of all its objectives' maturity rates (**Error! Reference source not found.**).

Identified M <sup>2</sup> HCS Domains	Sum of Objectives' Ratings/ Number of Objectives in a Domain	Ratings of Domains
Incident & Response Management	16/5	3.2
Identity Access Management	8/3	2.7
Enterprise Risk Management	14/5	2.8
Personnel Security	16/5	3.2
Physical Security	16/5	3.2

**Table 6.8 Maturity Ratings for Each Domain**

Afterwards, the overall maturity level for all the domains in the proposed maturity model was calculated. The overall maturity level is the average of the maturity of all the domains.

The final maturity level was calculated with this formula:  $\beta = \sum_{d=1}^n (L_d)/n$

where  $\beta$  denotes final maturity level,  $\sum$  denotes summation of domain levels,  $d$  denotes domain,  $L$  denotes level for each domain, and  $N$  denotes numbers of domain. The final maturity level obtained from the assessment of this case study is

$$\beta = \sum(3.2+2.7+2.8+3.2+3.2)/5 = 3.02 \approx 3.$$

Stage 6: This stage checked for additional information obtained; there was none in this case study, so the process proceeded.

Stage 7: A list of practises was proposed to support the hospital in its progress in the maturity rating of its electronic healthcare cloud security (OC6). Using the M<sup>2</sup>HCS maturity model matrix, security practises above their current ratings were reviewed in line with their resources to develop their progress (OC7).

Stage 8: The progressive practises were placed in order of implementation to produce improved security policies and processes in the healthcare organisation. This was achieved using the method proposed in section 6.4.4 (OC7).

Based on these processes, legal requirements, and best practises, a set of recommendations was made to offer mechanisms for improving their maturity. It is important to note that the assessment also considered the case study's security policies and mechanisms defined to implement the policies. This allowed the organisation to assess the effectiveness of its security policies and improve them.

#### 6.4.4 Improving Maturity

By evaluating current cybersecurity abilities using M<sup>2</sup>HCS, the case organisation can determine its main concerns to promote its progression along the maturity model. It is likely that a healthcare organisation will need to take incremental steps in its maturity progression because there are finite resources available. The hospital could use the following method for progression:

- ⇒ Define selected capability domain, e.g. incident response management.
- ⇒ Choose control within capability domain, e.g. data governance.
- ⇒ Define accessible resources for improvement.
- ⇒ Understand defined processes needed to move the healthcare organisation from one maturity level to the next; e.g. to get from level one to two for data governance, the healthcare organisation must have their data mostly centralised and bureaucratic.
- ⇒ Develop an action plan to fulfil maturity criteria.
- ⇒ Implement the action plan.
- ⇒ Refine as needed.

The M<sup>2</sup>HCS cybersecurity assessment model provides a reusable process for any healthcare organisation to employ. It is possible for an organisation to advance in more than one domain at once.

#### 6.4.5 Presentation of the M<sup>2</sup>HCS Framework Prototype

As part of the practical validation, the researcher went further to test the practicality of the research findings in the formulated case study. Therefore, the case study was further used to observe the feasibility of using the maturity model for healthcare cloud security. To do this, the M<sup>2</sup>HCS framework prototype was designed and developed to support stakeholders in evaluating cloud security practises in their healthcare organisations, based on the proposed maturity model and assessment matrix. This proposed prototype (OC5) was intended for testing purposes; however, its potential is extensive, and it can be used to:

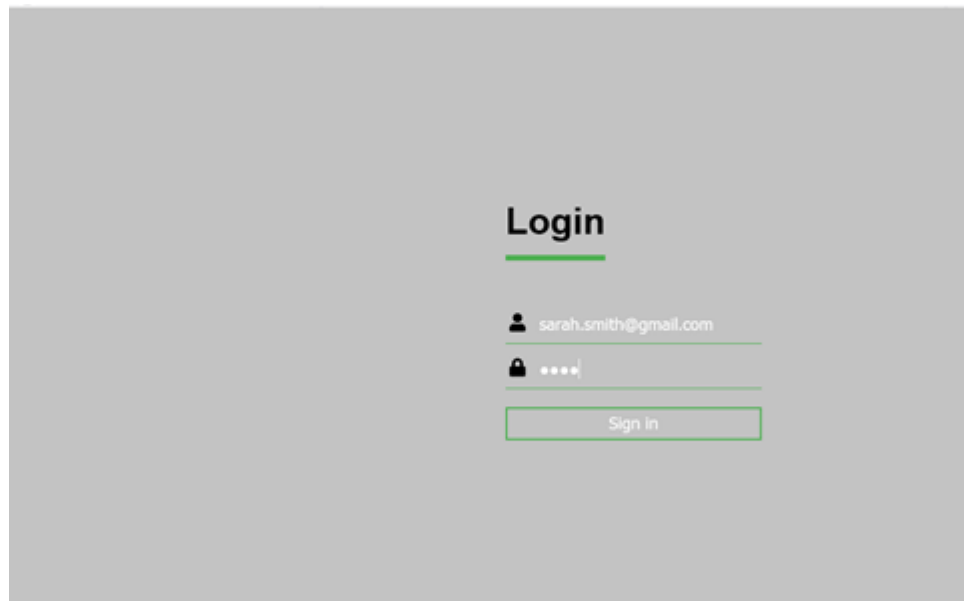
- ⇒ Support stakeholders in their decision making related to eHealth cloud security practises
- ⇒ Inform stakeholders about the existing level of maturity of their eHealth cloud security practises in their healthcare organisations
- ⇒ Inform stakeholders about the strengths and weaknesses when assessed by each domain of the maturity model
- ⇒ Allow stakeholders to improve maturity of eHealth cloud security practises by recognising their target level and processes for improvement

The proposed prototype was developed using WAMP, a software stack that consists of Apache 2.4.37—PHP 5.6.40, 7.0.33, 7.1.26, 7.1.30, 7.2.19, 7.2.14, 7.3.1, 7.3.6—MySQL 5.7.24—MariaDB 10.3.12—PhpMyAdmin 4.8.4—Adminer 4.7.0—PhpSysInfo 3.2.10 on Windows operating system. A Windows web development software allows creation of web applications using a virtual server,

saving the need for hosting. Apache is the server software responsible for serving web pages. When a page is requested to be seen, Apache grants the request over HTTP and shows the site. MySQL is the database management system for the Apache server. It stores all of the relevant information like the site's content, user profiles, and so forth. PHP is the programming language that acts like glue for the software stack. PHP runs by combining with Apache and communicating with MySQL (Bourdon, 2019).

Furthermore, the plan of user-friendly interfaces was considered in this study to improve the usability of the pages, but this was not the focus. The key screenshots of the prototype are accessible below for illustration. These screenshots provide information about the procedure, which entailed the use of the proposed device functions. The prototype of the M<sup>2</sup>HCS framework is as follows:

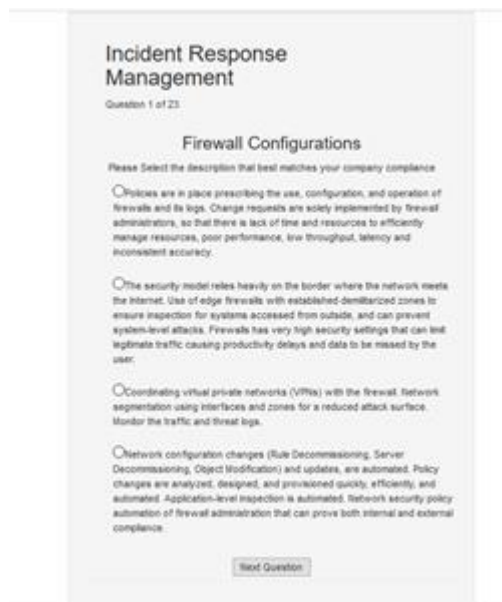
⇒ Create account and user sign-in using username and password to access the M<sup>2</sup>HCS framework prototype (Figure 6.2).



The screenshot shows a login interface with a light gray background. On the right side, the word "Login" is displayed in a bold, black font, underlined with a green line. Below it, there are two input fields: the first contains the email address "sarah.smith@gmail.com" and is preceded by a person icon; the second contains four dots and is preceded by a lock icon. A green "Sign in" button is located below the password field.

**Figure 6.2 Screenshot of the Login Form**

⇒ Start the assessment process (Figure 6.3).



The screenshot displays a questionnaire titled "Incident Response Management" with the subtitle "Question 1 of 23". The specific question is "Firewall Configurations", which asks the user to "Please Select the description that best matches your company compliance". There are four radio button options, each followed by a descriptive paragraph of firewall configurations. At the bottom of the question area, there is a "Next Question" button.

**Figure 6.3 Sample of Assessment Process**

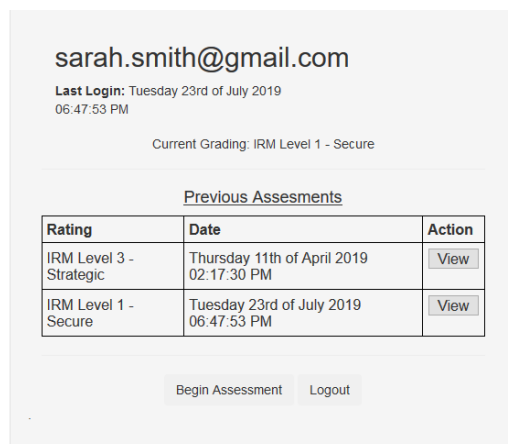


⇒ Present the results of the healthcare cloud security assessment and proffer ways of how to improve each domain (Figure 6.4).



**Figure 6.4 Result Page of the Assessment**

⇒ Table with link to access details of previous assessments (Figure 6.5).



Maturity Model for Healthcare Cloud Security (MMHCS)

**Figure 6.5 Previous Assessment Results**

This prototype was developed to further validate the viability and validity of the proposed maturity model.

## 6.5 Academic Peer Review

Academic peer review is considered the foundation of academic publication and communication. 'It is the practise of engaging relevant experts to read and provide a critical review on new research in the academic fields which they study to validate and endorse its contribution to knowledge'. Peer review maintains the excellence and validity of individual articles and the journals that publish them. It is an indispensable tool for making distinctions between what is truly scientific and what is speculation (Kelly, Sadeghieh and Adeli, 2014).

A number of research outputs were produced alongside the study course. These outputs were submitted for academic peer review, which further buttresses the validation of the research outputs. Each of these research outputs is directed to a certain set of research objectives, as indicated in section 1.3.

The three research outputs (**Error! Reference source not found.**) serve as evidence of external justification. The researcher (Balogun and Papadaki, 2018), under supervision of Maria Papadaki, was presented to an international audience at the annual ICITST Conference (13<sup>th</sup> International Conference for Internet Technology and Secured Transactions) in the United Kingdom in December 2018. This paper was extended into and accepted as a journal article (Akinsanya, Papadaki and Sun, 2019b). Another paper by the researcher is a result of the literature review study of M<sup>2</sup>HCS development (Akinsanya, Papadaki and Sun, 2019a), which was accomplished under the supervision of Maria Papadaki. It was presented to an international audience at the annual CERC conference (9<sup>th</sup> Collaborative European Research Conference) in Germany in March 2019. The

M<sup>2</sup>HCS model was accepted and published as an original research paper to the *International Journal of Information and Computer Security (IJICS)*.

Title	In-text reference	Type of output
Organisational Factors Influencing Medical Data Sharing in Cloud	Opeoluwa Akinsanya (2018)	International conference presentation
Factors Limiting the Adoption of Cloud Computing in Teleradiology (Extended Version)	Opeoluwa Akinsanya (2019)	Academic journal (online)
Current Cybersecurity Maturity Models: How Effective in Healthcare Cloud?	Opeoluwa Akinsanya (2019)	International conference presentation
Towards a Maturity Model for Healthcare Cloud Security (M <sup>2</sup> HCS)	Opeoluwa Akinsanya (2019)	Academic journal

**Table 6.9 Research Outputs: External Validation**

## 6.6 Limitations of the Study

Several factors would need to be considered before completely approving this methodology as a general methodology for healthcare cloud security maturity assessment. First, the case study was developed from policy documents, which may not reveal the real-life practises in the healthcare organisation. Secondly, the researcher has not considered the healthcare cloud security maturity assessment of observed organisations with other methodologies, tools, or approaches for healthcare cloud security maturity assessment to compare the outcomes. Lastly, the methodology has not been applied or validated in a real-life healthcare organisation's cloud security assessment practise, which is

planned by the NHS Trust University Teaching Hospital and occurs several times per year, controlled by different incidents and audit activities or the Board.

## **6.7 Chapter Conclusion**

This chapter presented and discussed the validation of the maturity model for healthcare cloud security (M<sup>2</sup>HCS) in view of the collected feedback. To conduct the validation process, these involved the demonstration and assessment of a case study to test the model's real-life application. Afterwards, steps to improve the maturity of the case study were presented. Surveys and resulting interviews were used to gather experts' feedback on the assessment of the maturity model. Prior to this, the backgrounds of the study participants were presented and discussed to reveal their suitability for this validation. Other strategies used were academic peer reviews from scientific publications. This validation has been successfully performed, as shown in the validation feedback from the experts that informed changes and improvements to the maturity model's matrix.

## **Chapter Seven**

### **7 Research Overview**

This study has gone from identifying the main factors limiting the adoption of cloud computing for healthcare, which were mainly realised to be organisational applications of the security solutions, to reviewing cybersecurity maturity models that can be effective for assessing security applications within healthcare organisations actively using cloud computing. The central concerns identified are that most security maturity models were solely assessing compliance to a standard, which, in effect, does not provide an objective assessment result. In addition, security maturity models were only assessing individual IS components, which, in effect, does not reveal the overall security posture of the healthcare organisation. Therefore, in this thesis, the maturity model for healthcare cloud security is discussed as a holistic tool that incorporates sub-domains of healthcare security practises. This requires comprehensive healthcare organisational security strategy and programmes, which can be multifaceted but not necessarily appropriate for their cloud environments.

However, in the literature, there are very few studies reporting on data governance for cloud service, despite its significant importance. Following this, the objective of the study was to create a more holistic model that can be used to produce and support a healthcare organisation's security practises against cyberattacks, specifically in the cloud environments.

To fulfil the research objectives, the study used the foundational capability and security maturity models (Savvides, 2009; NHS, 2011a; Spruit and Röling, 2014;

Giokas, Sekhon, Mestre, Geffen, Nouri and Twoekowski, 2015; Giokas, Sekhon, Mestre, Geffen, Nouri and Tworkowski, 2015; Le and Hoang, 2017) since they are well-known and tested models in cybersecurity and healthcare environments. They provided a well-defined, continuous approach for processes' improvement and assessment. The novel contribution of the proposed model aims to support healthcare organisations in developing the maturity of their security practises against emerging cyber and cloud security attacks. Furthermore, it assesses the usability and functionality of the implemented security practises within each domain and the workflow of the healthcare organisation. The model is conceptualised at a high level, focussing on the characterisation of the maturity goals of cybersecurity for healthcare organisations using third-party or their own cloud services. The model allows assessment of present cybersecurity abilities and defines the main actions each healthcare organisation must perform to progress along the maturity curve to attain the optimisation stage.

The research was conducted using Design Science Research Methodology, DSRM since its purpose was to construct and validate a healthcare cloud security maturity model (Hevner *et al.*, 2004). The research process involved the analysis of relevant literature using a systematic approach, and the validation strategies included a demonstration using a case study based on the policy documents of an NHS Trust University Teaching Hospital to ensure the applicability of the maturity model in a real-life environment, collection of experts' feedback on their assessment of the maturity model using survey questionnaires, and resulting interviews of survey participants. The feedback from the surveys and interviews was used to further improve the maturity model's matrix. Another validation

strategy was academic peer review through submission to scientific publications. The combination of the foundational maturity models, methodology, and validation strategies have all supported a rigorous research process that resulted in solid findings, meeting all the thesis objectives.

## **7.1 Communication**

This section relates to the communication step of DSRM that entails communicating to the appropriate audience the research on developing the maturity model, M<sup>2</sup>HCS, and its contributions. To communicate about the maturity model, the researcher wrote for scientific publications. This was also accomplished through the submission to a scientific journal and an international conference, as seen in section 5.6.

The first paper is based on the literature review results, which is the first step of this research, in which the researcher identified the main issues affecting the current cyber security maturity models and the foundational maturity models for the proposed model. The second paper presented the development processes and case study validation of the proposed maturity model, M<sup>2</sup>HCS, based on the policy documents of a UK NHS Trust University Teaching Hospital.

## **7.2 Research Contributions and Findings**

The research process has led to a number of findings and contributions to knowledge. The main ones include the following:

- ⇒ Findings about eHealth cloud's potential benefits to meet challenges for healthcare provisioning include support for patient-centricity healthcare service, real-time availability of data regardless of the geographical

locations and time difference, fostering collaboration amongst healthcare inter-organisations, information synchronisation and simultaneous sharing, and clinical research by providing computing storage. All these are based on the features of cloud.

⇒ Findings from conducted interviews about limiting factors in the adoption of cloud in healthcare presented technical, organisational, and legal challenges. The technical challenges include:

- Data and service reliability, data and service availability, disaster recovery, transmission speed, web performance and latency, integration and interoperability, data portability and quality, and access control solutions suitable for clinical workflow.
- Amongst these, the performance, reliability, and availability were considered crucial for medical practitioners, who cannot effectively operate unless their applications and patients' data are available.
- It is noteworthy that the technical cloud architects (TA1) type of cloud service providers provided the required technical security solutions for their data centres.

⇒ Findings about the organisational challenges included organisational changes, end users' trust, and costs.

- Costs were stated to be the crucial factor; these include the financial investments required to develop, implement, and maintain the eHealth cloud. Lack of service costs for required performance and high initial costs mainly deter the adoption of eHealth cloud.



⇒ Findings about the legal challenges include contract law, intellectual property rights, data jurisdiction, and privacy.

- Data jurisdiction was stated to be the major concern. There are limited legislations and guidelines for clinical, technical, and business practises of healthcare security practises in cloud.
- Overall, the organisational challenges regarding the implementation of technical solutions were identified as the major limiting factors in adopting eHealth cloud. This overall finding, otherwise considered the initial research gap, defined the direction for the research onwards.

⇒ Findings from the study revealed the research is timely since there is presently a financial crisis such as 'rising cost to provide healthcare services in the United Kingdom' (Shaw, 2018). This study asserts that the adoption and implementation of eHealth cloud would reduce huge financial debts faced by many healthcare trusts.

⇒ Findings from the systematic review of foundational maturity models revealed the research gaps within the literature, addressed by the proposed model, M<sup>2</sup>HCS, include:

- The lack of a security maturity model streamlined for eHealth cloud.
- The other identified gaps in the review of these maturity models are in the aspect of adoption; the maturity models either are too complicated to implement or require the healthcare organisation's processes to be refined to suit the model's implementation.

- ⇒ The novel contribution of this research is the proposal of the model. M<sup>2</sup>HCS, which is a high-level, holistic model that can be used to support and promote a healthcare organisation's usable security practises against cyber and cloud security attacks.
- It possesses five core indicators or domains: identity and access management (IAM), Incident response management (IRM), enterprise risk management (ERM), personnel security (PeS), and physical security (PhS). They address comprehensive features of cloud security.
  - M<sup>2</sup>HCS also incorporates usability and functionality objectives into its assessment of security practises to ensure usable security solutions are implemented.
  - M<sup>2</sup>HCS can support the assessment of security practises in the eHealth cloud (OC1).
  - M<sup>2</sup>HCS metrics can be followed easily and intuitively (OC2).
  - M<sup>2</sup>HCS descriptions of the objectives are clear and relate to the maturity levels (OC3).
  - M<sup>2</sup>HCS supports the assessment of the maturity of the each of the specified domains to identify weak and strong practises (OC4).
  - M<sup>2</sup>HCS can aggregate results from the individual domains to a suitable output that can be understood by all stakeholders (OC5).
  - Further steps towards improving the maturity level are recommended (OC6).

- Recommendations should be prioritised for improving the maturity based on available healthcare organisational resources (OC7).
- ⇒ The concise summary of the assessment activities is a guide for good practises and validation. M<sup>2</sup>HCS metrics support a qualitative and quantitative assessment of the cloud security in the healthcare organisation. These can be used for intra-organisational eHealth cloud security observation over time, progress made by the organisation's policies, and the attainment of a goal recognised through the study of similar healthcare organisations' cloud security proficiencies.
- ⇒ The maturity progresses through four levels, from reactive to compliant, proactive, and resilient. Maturity levels specify the advancement of maturity to achieve a considerably (highly) secure level of eHealth cloud system. Each level has a predefined set of characteristics.
- Level 1 is characterised by having elementary practical eHealth cloud security implementations; it is unreliable and has *ad hoc* implementations.
  - Level 2 is characterised by having security mechanisms focussed on essential systems to provide a level of stability and perception that their systems are protected.
  - Level 3 is characterised by having security policies and procedures implemented with suitable mechanisms to support awareness and compliance.

- Level 4 is characterised by having control over the security needs of the healthcare organisation. The priority of physical security is considered the same as of cloud security.

⇒ The validation authenticates the contribution of the proposed maturity model, M<sup>2</sup>HCS, as well as its usefulness, value, capability, and operational characteristics. A validation strategy was developed to provide a convincing argument for the model's effectiveness and demonstrated its function within its proposed and realistic environment. It included the use of a case study, online surveys/interviews, and peer review from the scientific community. Results ascertained that M<sup>2</sup>HCS offers a suitable and strong progression method and is dependable when it comes to improving functioning healthcare cloud security.

- Findings from the case study revealed all of the operational characteristics (OC) were attained, except OC5. The case study was assessed using the M<sup>2</sup>HCS metrics framework and formula to reveal an overall maturity level of 3. A list of steps was offered for improving their maturity.
- Feedback from surveys and interviews revealed that the proposed model has the capability to follow its stages, through its proposed objectives and domains, amongst all the other operational characteristics attained. Further refinements were made to the model based on this feedback.

- Publications of research results in written form and reviews from the scientific community revealed that the research findings contributed knowledge to the field.
- The prototype was used to attain the operational characteristic (OC5).

⇒ The proposed maturity model, M<sup>2</sup>HCS, has extensive potential to:

- Support decision makers in their healthcare organisation's cloud security practises assessment
- Enlighten decision makers about their present security practises' maturity
- Educate decision makers about their strong and weak security practises
- Provide recommendations to improve their weak practises
- Prioritise their recommendations based on available resources

### **7.3 Research Limitations**

Even though the thesis has fulfilled all research objectives, the researcher recognises some limitations which could be addressed in future work, especially considering that this research is the first study to focus on cloud security assessment for healthcare. Whilst the few preceding studies have been an advantage in developing a highly novel research this can also be considered a limitation. The research findings could have been improved with richer literature, resulting in more recognised metrics and models which would have reinforced the research direction for this thesis. On the other hand, the limited number of

preceding studies has given the researcher the chance to create some important practicalities in the area of eHealth cloud security assessment, with an invaluable contribution to knowledge.

A different limitation is connected to the research methodology, mainly for the validation of the thesis. This is a known drawback in all research projects which employ surveys and is related to the bias in the participants' responses and the limited sample population. In this research, the number of participants was limited for the project; however, it involved balanced representations. A larger sample population with more representations of the relevant participants would have strengthened the research findings.

The last limitation of this study is associated with time and resource constraints; this paper had to be completed within a reasonable timeframe allocated for PhD research. If more time was allocated for the validation work, the level of detail obtained, particularly from the survey and interviews, would have been greater and of a wider scope.

#### **7.4 Recommendations for Further Research**

eHealth cloud security assessment and maturity models are a fairly novel phenomenon, and this research serves as an initial point for further study into this field. Many prospects have been discovered and are considered worthy of future research. Recommendations for this are as follow:

- ⇒ Demonstrate that the model can be used regardless of the differences amongst the eHealth cloud models (IaaS, PaaS, and SaaS).

- ⇒ Extend the validation of the research findings in this thesis to all other healthcare organisations.
- ⇒ Investigate eHealth cloud security assessment for diverse case studies and practical demonstrations in many countries, which will allow opportunities for assessment amongst these nations and implementation of best practises.
- ⇒ Individual elements of the proposed model in this thesis could be a standalone research project, which allows for in-depth, e.g. IAM, assessment of eHealth cloud and end users' trust assessment of eHealth cloud.
- ⇒ The proposed metric framework for assessment has a vast potential that can be extended to an automated framework system for customised eHealth cloud security assessment programmes, based on a healthcare organisation's requirements.
- ⇒ The merging of the Internet of Medical Things (IoMT) with the cloud has been a subject of research interest. It is suggested that such a merging carries huge potential, along with some challenges too. There is an agreement that privacy and security are its key concerns. A major challenge is the lack of mature security for healthcare data within such a merged environment. This creates opportunities for important research to address the challenge of eHealth cloud security assessment of an IoMT ecosystem.

## **7.5 Conclusion**

This chapter presented and discussed an overview of the study, from identifying the major factors limiting the adoption of eHealth cloud to reviewing cyber security maturity models that can be effective in assessing applications in eHealth cloud. It also discussed the development of the proposed model, M<sup>2</sup>HCS, and its validation strategies.

Research contributions and findings were presented, along with the key contributions to this area of knowledge. The study, despite fulfilling all research objectives, has limitations that were identified and discussed. Lastly, recommendations were provided for future research in related subjects.



Appendices

Appendix A1 - M<sup>2</sup>HCS detailed matrix (IAM)

IDENTITY & ACCESS MANAGEMENT LEVEL 1				
	CONTROL	OBJECTIVE	DESCRIPTION	CORE
	Authorization and Access control	IAM.1.2	Relies on single factor authentication. The authentication platform reacts report on what users are accessing. Focus is on increasing the strength of the password. Have patchworks and silos of IAM of the healthcare organization's IT. Consistently allow the least privilege required.	YES
	Automatic logoff of system users		Users remain logged on no matter how long they may be inactive, except they manually log off the system, or kill off the granted session. After defined unsuccessful attempts to log on, the user is locked out of the system and the IT administrator must reinstate the user's access.	
	Mobile device management		Traditional monolithic management - dealing with mobile device management issues by standardizing on a single style of device and implementing a complete mobile device management infrastructure. Mobile network wireless connections use weak encryption protocols.	
	Identity Federation & Provisioning	IAM.1.1	Use of authentication and authorization information for a cloud service consumer across multiple cloud services or cloud-based IT resources, if need to be invoked as part of the same overall runtime activity.	YES
	Usability & Functionality		Standardized, reliable credentials and identity media in widespread media use. Provide help documentation	

IDENTITY & ACCESS MANAGEMENT LEVEL 2			
CONTROL	OBJECTIVE	DESCRIPTION	CORE
Authorization and Access control	IAM2.2	Healthcare organization has an access control policy governing access to personal health information. Level of authentication required of user identity is consistent with levels of access. Adoption of alternative authentication technologies. Implement cloud-based endpoint security platforms. Define and integrate identity provisioning into cloud deployment. Perimeter security for lower level network defense and higher level defenses against application attacks.	YES
Automatic logoff of system users		System administrators configures systems to ensure that users are automatically disconnected when idle for one hour. Determine the threat level for your hospital and balance that against the cost of your Help Desk support for password resets. Potential of setting the account lockout duration too high.	
Mobile device management		Ensuring the right controls are on the device and putting the correct policies and procedures are in place. Deploying technology on the network that allows you to interrogate devices that are attempting to connect and identify them and have the right controls and anti-virus protection in place on the device. Information on mobile devices are not always backed up.	
Identity Federation & Provisioning	IAM2.1	Knowledge-based authentication for remote identity proofing. Capabilities that allow the management of privileged user access to cloud services and provide session recording. Audit access to cloud services. Audit should provide record each time and uniquely identify	YES
Usability & Functionality		Enable enhancements to protect evolving threats, and attributes for accountability. Visible security state and accessible functions	

IDENTITY & ACCESS MANAGEMENT LEVEL 3			
CONTROL	OBJECTIVE	DESCRIPTION	CORE
Authorization and Access control	IAM3.2	User registration details are periodically reviewed. Segregate duties and responsibilities to reduce unauthorized abuse of personal health information. Access control is based on predefined roles with associated authorities consistent with the needs of the role. Implement federated identity management solution. Define privilege users requirements using higher levels of assurances in emergency situations. Manage identities across applications, devices, and systems. Implement provisioning for identities and cloud service provider. Secure mechanisms for users to authenticate using cryptographically valid and well documented standards.	YES
Automatic logoff of system users		Implement electronic procedures that terminate an electronic session (automatically log off and lock the computer when idle, force-response timeout, or disconnect remote session) after a predetermined time of inactivity. Enable the mobile device time-out or automatic logoff feature. Implement self-service password resets that relies on security questions, the capability to email or text new passwords to end users, and multi-factor authentication, so users must verify their identities before proceeding	
Mobile device management		Perimeter is being extended to many different 'selected' mobile devices. Ensure data loss prevention to limit where patient data can be obtained live and how much data is wanted on these mobile devices. Protect the data transmission between devices and create a gateway to view and use information without retaining it	
Identity Federation & Provisioning	IAM3.1	Just-in-time provisioning during user federated Single Sign-On. Enhanced administration model to better manage federations to the cloud. Record of former data/information prior to update is retained.	YES
Usability & Functionality		Identity portability, use of various credentials in asserting their digital identities to service providers. Reduced cognitive load on users memory	

IDENTITY & ACCESS MANAGEMENT LEVEL 4			
CONTROL	OBJECTIVE	DESCRIPTION	CORE
Authorization and Access control	IAM 4.2	Authentication to process personal health information should involve strong authentication using multiple factors with federation. IT systems contain application functionalities that enforce the approval of clinical processes by roles. Focus is to make the user identity technologies more secure, personal, and usable. Higher-level security access processes such as smart card based access, single sign on capability. Ensure cloud service provider implements strong metastructure security. Robust logging and monitoring of administrative alerting of unusual events.	YES
Automatic logoff of system users		The system is configured to automatically sign off all the computers when a remote control session is disconnected. This additionally removes cached data from the computers. When a defined number of unsuccessful attempts have been attempted, the system should have the ability to disable the account or terminal for a certain amount of time or until verification of reason for lockout. A robust auditing mechanism is in place to alert administrators when a series of failed logons are occurring immediately and urgently	
Mobile device management		Automating the process to locate, lock, and potentially wipe lost devices. Use of geofencing capability which can generate alerts and take action should a device cross a specific boundary. Automated process of enrolling devices and users.	
Identity Federation & Provisioning	IAM 4.1	Authentication is driven by standards-based token exchange while the user directories remain in place within the centrally administered domain as opposed to synchronized externally. It addresses secure connection to multiple applications (web browser, and downloads and installations on mobile devices) outside of the hospital perimeter. Audit records are tamper-proof and secure.	YES
Usability & Functionality		Identity solutions that are privacy enhancing, voluntary, interoperable, secure, resilient, cost effective, and easy to use. Security does not inhibit or reduce workflow	

## Appendix A2 - M<sup>2</sup>HCS detailed matrix (IRM)

INCIDENT RESPONSE MANAGEMENT MATURITY LEVEL 1				
Control	Objective	Description	Core	
Firewall configurations		Policies are in place prescribing the use, configuration, and operation of firewalls and its logs. Change requests are solely implemented by firewall administrators, so that there is lack of time and resources to efficiently manage resources, poor performance, low throughput, latency and inconsistent accuracy.		
Disaster Recovery/Business Continuity		Use of widely accepted IT model for disaster recovery. A cloud disaster recovery strategy that requires adjustment for the ever-changing healthcare conditions and environmental changes. Look at historical performance of cloud service provider. There are tools and techniques to keep cloud deployment running if it breaks. Takes risk-based approach. No viable recovery strategy.		
Incident Response & Containment	IRM 1.2	Incident response is reactive. Preparation of incident response guidelines and disclosure obligations 'least privilege'. Including the cross-border nature of cloud computing. Standards compliance-driven. Establish security incident management responsibilities and procedures.	YES	
Usability & Functionality		Focus is on what users need to be able to do, not technical implementation that will allow them achieve it. Organizational goals-focused and not feature-focused		
Incidents Reporting management		Contract does not commit providers to reporting about security incidents to hospitals. Complex taxonomies or list of incidents that would change over time is developed and used for reporting. There is no set threshold for parameters to be reported.		

INCIDENT RESPONSE MANAGEMENT LEVEL 2			
CONTROL	OBJECTIVE	DESCRIPTION	CORE
Firewall configurations		The security model relies heavily on the border where the network meets the Internet. Use of edge firewalls with established demilitarized zones to ensure inspection for systems accessed from outside, and can prevent system-level attacks. Firewalls has very high security settings that can limit legitimate traffic causing productivity delays and data to be missed by the user.	
Disaster Recovery/ Business Continuity		Strategy focuses on major disasters, disaster recovery based around replicating virtual machines to a remote data centre or cloud. Priority is accorded to business continuity management. Business continuity plans focuses on healthcare crisis management. Prepare for portability in case of need to migrate service providers or platforms. Leverage business continuity/ disaster recovery features for platforms. Design your applications to gracefully fail in service outage.	
Incident Response & Containment	IRM 2.2	Automated workflows to handle alerts, review of response actions taken. Incident response plan covers business associates and other organizations that hospital make transactions with. Several/Layered solutions-driven. Exchange of information across trans-border involve minimum set of controls to be implemented. Quick, effective and orderly response to security incidents.	YES
Usability & Functionality		Investigate solutions that 'does the right things well', with a combination of features in line with identified requirements. Solutions that are already in use by other healthcare organizations with similar mandates	
Incidents Reporting management		Document agreed terms and protocols to meet responsibility and liability. Clear roles and responsibilities for incident reporting team. Periodic training using test scenarios and functional training for all activities within the programme. Effective escalation path for incidents.	

INCIDENT RESPONSE MANAGEMENT LEVEL 3			
CONTROL	OBJECTIVE	DESCRIPTION	CORE
Firewall configurations		Coordinating virtual private networks (VPNs) with the firewall. Network segmentation using interfaces and zones for a reduced attack surface. Monitor the traffic and threat logs.	
Disaster Recovery/ Business Continuity		All personal health information are backed up and stored in physically secure environment. Frequent testing of cloud disaster recovery plan and backup, while continuing to protect production systems. Regular audit and record of former content prior to update is retained. Business Continuity plans are suitably integrated with healthcare organization's plans for dealing with emergencies. Prepare for wider outages that take down service provider outside the capabilities of inherent controls. Ensure real-time switching in service outage.	
Incident Response & Containment	IRM 3.2	Operationalize breach responses by incorporating elements of incident response plan into daily processes and business practices. Design of pilots for interrogation of all events and establishing alert thresholds. Vulnerability-driven. Artificially separate information security incidents from other types of incidents handling	YES
Usability & Functionality		The interfaces are intuitive, aesthetic, and offer streamlined workflows. Implemented solutions are affordable to maintain	
Incidents Reporting management		Ensure relevant metrics are used to collect evidence, and evidence collected is good, forensically and legally correct. Use of functional and forensics techniques for quarantining, real time observation, investigation, analysis, and reporting of incidents. Collect and preserve incident-related data.	

INCIDENT RESPONSE MANAGEMENT LEVEL 4			
CONTROL	OBJECTIVE	DESCRIPTION	CORE
Firewall configurations		Network configuration changes (Rule Decommissioning, Server Decommissioning, Object Modification) and updates, are automated. Policy changes are analyzed, designed, and provisioned quickly, efficiently, and automated. Application-level inspection is automated. Network security policy automation of firewall administration that can prove both internal and external compliance.	
Disaster Recovery/Business Continuity		Timely backups and replication between on-premises workloads and disaster recovery destination. Use of multiple cloud disaster recovery strategy. Physical removable media has information encrypted against abuse, and protected from theft. Audit records are tamper-proof and secure. Business continuity plans are regularly tested on programmatic basis. Improved resilience options that is beyond what is attainable in traditional infrastructure. Design for Recovery Time/Point Objectives equivalent to those on traditional infrastructure. Use chaos engineering to continuously test business continuity.	
Incident Response & Containment	IRM.4.2	High state of readiness and run tests continually. Integrate incident response with culture of continuous improvement so that new response mechanisms are developed. Update policies and procedures to include mobile devices and cloud services. Innovation and threat modelling-driven. Evaluate effectiveness of established controls.	YES
Usability & Functionality		Focus is on advanced detection and incident management methods with customizable capabilities, and integration into workflow systems	
Incidents Reporting management		Cloud security incident reporting includes bi-directional sharing schemes, where authorities feedback analysis and statistics to providers. Hospitals addresses incident reporting in their contracts and SLAs. The thresholds of the parameters are developed by the hospitals and reported. A single framework for reporting by providers and hospitals is used. Incident report displays incidents in the various layers of cloud services. Information security assessment is made on all incidents or representative incidents.	



## Appendix A3 - M<sup>2</sup>HCS detailed matrix (ERM)

ENTERPRISE RISK MANAGEMENT LEVEL 1			
CONTROL	OBJECTIVE	DESCRIPTION	CORE
Event identification		Hospital requires contractors to assess potential risks and vulnerabilities to ePHI in a patchwork fashion.	
Risk assessment & response	ERM 2.2	Identify the systems, subsystems, components and subcomponents that are most essential to healthcare operations and hospital's environment. Obtain information, use security frameworks, with defined requirements, to aid the adhoc risk assessment process with no scope	YES
Information Assurance		Embrace and aid the on-going deployment of information confidentiality, integrity, and availability. Low quality data has a negative impact on the accuracy or timeliness of the hospital's decision making. Data is too little, decentralized, inconsistent, and uncoordinated across clinical departments. Multiple, distributed analytic systems. There is governance gap. Merely new technical protections. Information architectures are fractured.	
Risk management	ERM 2.1	Manages overall risks for the healthcare organization. Outsources overall responsibility and accountability for risk management to cloud service provider. Existing traditional governance and risk management activities are directly transferred to the cloud, ignoring new cloud computing complexities relating to the underlying components. Has a blanket risk decision about cloud service provider.	YES

ENTERPRISE RISK MANAGEMENT LEVEL 2			
CONTROL	OBJECTIVE	DESCRIPTION	CORE
Event Identification		Establish in daily practice critical hospital-wide risk management preparatory activities to facilitate a more effective, efficient, and cost-effective execution.	
Risk assessment & response	ERM 2.2	Hospital identifies controls, processes, and technology solutions to fortify recommendations and establish reasoning for costs. Value the importance of assets and their relations. Assess the impact of an possible incident by developing incident scenarios. Assess the likelihood of an possible incident by the importance of the risks and their priority	YES
Information Assurance		Exploit decision support technologies and trends to evidence-based healthcare. Hospitals will either over-apply data governance for the new function, or under-apply data governance due to lack of experience. Data is too centralized, and bureaucratic. Monolithic early binding data model. Responsibilities and mechanisms for governance are defined. New approaches to fundamental governance. There's a recognized difference between data custodianship and ownership across teams. Ensure destruction and removal of data in accordance with policy. Ensure requirements, information management, and security policies align.	
Risk management	ERM 2.1	Aligned to the healthcare organization's governance and risk tolerance. Changes are made to existing traditional governance and risk management processes. Roles and responsibilities for risk management between cloud service provider and healthcare organization are defined. Healthcare organization is responsible for risks ownership.	YES

ENTERPRISE RISK MANAGEMENT LEVEL 3			
CONTROL	OBJECTIVE	DESCRIPTION	CORE
Event identification		Hospital not only conducts a comprehensive risk analysis, but also evaluates and addresses potential security risks when implementing enterprise changes impacting ePHI  Relationship between the risk management processes at the governance level of the organization and the individuals, processes, and activities at the system and operational level. Standards and guidelines have been identified to inform risk assessment activities. Authority and responsibility for the performance of the risk assessment is assigned to personnel. Results of regular risk assessment is aligned with the priority and resources of the healthcare organization. Risk assessment aligns with value and requirements of assets involved.	YES
Risk assessment & response	ERM 3.2		
		Integrate information governance to support clinical and corporate governance. Capable of quickly enforcing the changes required in source data systems and workflows that are necessary for raising data quality. Ensure personnel are literate about the interpretation and meaningful use of data as it applies to their role. Healthcare organizations adjust their processes to accept associated risks and close the gap. Additional controls may be implemented to restrict data to particular locations. Information classifications and management policies are adjusted for cloud computing. Information architectures are improved. Healthcare organizations are informed about the logical and physical locations of data.	
Information Assurance			
	ERM 3.1	Covers all sorts of risks from financial to physical. Good documentation for responsibilities and potential for untreated risks. Risk documentation provides information to aid effective risk decision. Build a matrix of cloud services with types of assets allowed in the services. Implement right controls for residual risks.	YES
Risk management			

ENTERPRISE RISK MANAGEMENT LEVEL 4			
CONTROL	OBJECTIVE	DESCRIPTION	CORE
Event identification		Conducts comprehensive risk analysis and implements corresponding risk management plan that will evaluate and address any weaknesses in the organizational structure.	
	ERM 4.2	Hospital takes a long-term approach to risk management while forming repeatable processes and standards. There is a framework in place to offer structure, strict objectives. The risk assessment is periodically reviewed. The risk assessor is experienced and well trained. The process is well documented. Top management support the risk assessment process. Stakeholders from different units are involved	YES
Risk assessment & response		Information security risk management is as equal in importance to care treatment plans, infection management strategies, and other clinical management matters. Data is consistent, well-documented and trustworthy. Ensure data-driven decision-making and data transparency around quality and cost. Multiple years strategy for data governance that maximizes healthcare data's value to the mission of their organizations. Distributed late binding data model. Healthcare organization performs cloud service provider assessments and audits on compliance reporting of cloud service provider. Information governance policies and practices fully align to the cloud.	
Information Assurance		It covers governance, technology, and process capabilities of cloud service provider. Protect the ability to validate risk as it relates to personal health information and applications. Periodical review assessments of cloud service provider's services to meet standards. Periodic assessments are scheduled and automated.	YES
Risk management	ERM 4.1		

## Appendix A4 - M<sup>2</sup>HCS detailed matrix (PeS)

PERSONNEL SECURITY LEVEL 1				
CONTROL	OBJECTIVE	DESCRIPTION	CORE	
Awareness training for all employees	PeS 1.1	The organization depends on staff to seek out knowledge on their own, or develops a structured approach without a critical mass of cloud knowledge. Staff lacks critical skills.	YES	
Third parties' security		Hospitals rely on the cloud service provider security processes. Service providers and contractors are given access to systems containing protected information or handle sensitive data sets. Managing cybersecurity incidents involving vendors is difficult		
Hospital Organizational culture	PeS 1.2	The chief information officers (CIO) and chief technology officers (CTO) have major influence in the cloud business transformation process, yet provide low management support. These leaders do not develop a digital vision and strategic plans to lead their hospitals into the new digital era of cloud computing. Slow adoption of new technologies and general aversion to risky innovations.	YES	
Usability & Functionality		Clinicians don't often have time to devote to effective usability testing, and the healthcare organization don't have usability as one of its top priorities, which means that it is not one of the organization's core values		
Human Resource		Staff are obliged to work under significant stress resulting to heightened error rates, and performance of incorrect procedures. Attention is on roles and responsibilities of short term staff.		

PERSONNEL SECURITY LEVEL 2			
CONTROL	OBJECTIVE	DESCRIPTION	CORE
Awareness training for all employees	PeS 2.1	Use of an internal/employee security awareness program. Implement security awareness campaign. Frequent training sessions. Use of on-demand security videos, newsletters with training materials and information on security tips, webinars with insights on the latest security threats and education about how to protect work and personal devices.	YES
Third parties' security		Hospitals need to know precisely what data is being shared with vendors and how it's being managed. Hospitals considers the other businesses that may be partnering with their vendors. When sharing data with vendors, hospitals ensures they're only sharing the necessary data. Hospitals ensures their vendors have the security measures in place to manage their own assets.	
Hospital Organizational culture	PeS 2.2	Business and technology stakeholders do exercise conflicts of interest on cloud security issues. Adoption of cloud computing does not yield their desired results. Cloud security is seen as a technology control function rather than integrating it into daily business processes.	YES
Usability & Functionality		Clinicians find the system very hard to learn, and do not get sufficient technical support while attempting to use the system	
Human Resource		Specify what rights of access staff will have to personal health information. Effective management of health IT systems that addresses patients' confidentiality.	

PERSONNEL SECURITY LEVEL 3			
CONTROL	OBJECTIVE	DESCRIPTION	CORE
Awareness training for all employees	PeS 3.1	A current and comprehensive employee training program. As policies change, employee training program has to be ongoing and evolving. Quarterly internal audits where phishing attempts occur frequently. Visual cues in the form of posters within the hospital to spread the message and yearly assessments for employees.	YES
Third parties' security		Hospitals compile a comprehensive inventory of data and privacy risks. Risk assessment is effective for management of third party's access to systems containing personal health information. Ensure that the vendor knows what the hospital expects from them as a partner from security perspective. Verify they have the appropriate privacy and security in place.	
Hospital Organizational culture	PeS 3.2	Cloud security is not an occasional concern but an everyday task for core business stakeholders at all levels, inside and outside the hospital. Communications among critical decision makers are open and frequent. Security protocols are integrated into daily business processes without creating operational challenges and frustrations.	YES
Usability & Functionality		Clinicians use the system to perform their tasks quickly, and their efficiency is improved. They do not need to remember lots of things while using the system to perform their tasks.	
Human Resource		Security roles and responsibilities are included in organization's security policy. Regular updates in all healthcare organization's security policies and procedures are provided to all employees and third parties.	

PERSONNEL SECURITY LEVEL 4				
CONTROL	OBJECTIVE	DESCRIPTION	CORE	
Awareness training for all employees	PeS 4.1	Design a curriculum to develop skills for every job role. Training programs enforce key expected behaviors to make sure staff and control owners understand how their actions work. Training compliance is tracked and monitored to ensure accountability and acknowledgement of these responsibilities.	YES	
Third parties' security		Hospitals ensure all service providers, contractors and third parties are thoroughly screened in proportion to the information classification level to be accessed, the business requirements and acceptable risk. They also ensure the right contractual protections are in place. Audit vendor's compliance with all the rules and regulations, and set up a system to manage relations and monitor its performance.		
Hospital Organizational culture	PeS 4.2	The stakeholders have no major influence in the cloud business transformation process, yet they provide high management support. They develop a long-term view of cybersecurity, with strategic road map and plans in place to adequately protect information assets and IT systems. There is trust among the stakeholders to support digitally resilient culture.	YES	
Usability & Functionality		Clinicians are satisfied with the system overall. They use the system while interacting with their patients. They trust the system to keep their patient's information confidential.		
Human Resource		As clinical staff 'rotate' and their access rights change. Termination of previous rights should be processed as the individual leaving the organization's employment. Terminate user access privileges immediately after all related transactions are completed. Additional guidance where the personal health information crosses jurisdictional boundaries.		



Appendix A5 - M²HCS detailed matrix (PhS)

PHYSICAL SECURITY LEVEL 1			
CONTROL	OBJECTIVE	DESCRIPTION	CORE
Connected Medical Device	PhS 1.1	Medical devices are still running on obsolete operating systems, and others were manufactured with significant vulnerabilities, such as embedded passwords in the software code. Life span of the connected medical devices in use is outdated and patch management process usually is a third party task to perform	YES
Cloud Storage security	PhS1.2	Use manual processes with limited use of software tools. Use security perimeters to protect areas that contain personal health information facilities supporting health applications.	YES
Usability & Functionality		Clinicians don't often have time to devote to effective usability testing, and the healthcare organization don't have usability as one of its top priorities, which means that it is not one of the organization's core values	

PHYSICAL SECURITY LEVEL 2				
CONTROL	OBJECTIVE	DESCRIPTION	CORE	
Connected Medical Device	PhS 2.1	Manufacturers conduct pre-market testing of medical devices. Hospital ensure this testing has taken place, among other requirements, such as vulnerability and patch management of devices. Hospital set and enforce policies and standards for medical device procurement.	YES	
Cloud Storage security	PhS 2.2	Adopt contextual-aware monitoring with installed monitoring software, use of software for monitoring the data centre environment, IT, data centre power, devices, and the data centre's environmental conditions. Use appropriate entry controls to ensure that only authorised personnel are allowed access.	YES	
Usability & Functionality		Clinicians find the system very hard to learn, and do not get sufficient technical support while attempting to use the system		

PHYSICAL SECURITY LEVEL 3			
CONTROL	OBJECTIVE	DESCRIPTION	CORE
Connected Medical Device	PhS 3.1	Hospital perform asset management to classify the devices and measure their risk to the network and patients. Port security through network access control solutions ensure that visibility and control, so all medical devices get onto the network passing through the proper channels.	YES
Cloud Storage security	PhS 3.2	Implement operational automation with installed monitoring and management software. Implement cloud-based data centre monitoring and management strategies for non-sensitive monitoring data.	YES
Usability & Functionality		Clinicians use the system to perform their tasks quickly, and their efficiency is improved. They do not need to remember lots of things while using the system to perform their tasks.	

PHYSICAL SECURITY LEVEL 4				
CONTROL	OBJECTIVE	DESCRIPTION	CORE	
Connected Medical Device	PhS 4.1	Implement advanced micro-segmentation or basic levels of network segmentation to logically separate medical devices from others. Deployment of a behavioral anomaly-based network solution, specifically designed for medical devices.	YES	
Cloud Storage security	PhS 4.2	Implement business optimisation with full automated processes and use of AI and advanced analytics. Implement cloud-based data centre monitoring and management strategies for their remote sites and distributed IT offices.	YES	
Usability & Functionality		Clinicians are satisfied with the system overall. They use the system while interacting with their patients. They trust the system to keep their patient's information confidential.		

## Appendix B - Research Ethics



14 December 2018

CONFIDENTIAL

Opeoluwa Balogun  
School of Computing, Electronics and Mathematics

Dear Opeoluwa

### ***Ethical Approval Application***

Thank you for submitting the ethical approval form and details concerning your project:

### ***Cloud Security Maturity Model for Healthcare Medical Records***

I am pleased to inform you that this has been approved subject to clarification of the following:

- Storage of data and information. 3.1 states "Although the researcher will know the participant's identity, all collected data will remain anonymous". Will all emails, interviews, recordings, etc be securely deleted and all identifiers be removed prior to storage of data? For the different types of information that may be collected, this is not entirely clear in 5.7. At what point will recorded data be anonymised for example? How will it be "stored securely" prior to that point?
- Modification of the information sheet is required as follows:

Ethical approval is not given by the School but by University of Plymouth Faculty of Science and Engineering Research Ethics & Integrity Committee.

Include information on what the research is to be used for i.e. in part fulfilment of your PhD at University of Plymouth (and any other use).

You have not indicated how the participants can withdraw should they choose to from the study. How is the consent going to be recorded? May be a box on the questionnaire with the statement that I give consent to take part in the study.

Finally, it will not take 15-20 minutes. It will probably take this long to complete the questionnaire as all responses will be typed and it is likely to take another 15-20 minutes to read the information sheet.

Kind regards



Paula Simson  
Secretary to Faculty Research Ethics Committee

Cc. Dr Maria Papadaki

## **Appendix C - Survey Information Guide**

Dear <participant name>,

Based on your expertise in the cloud security or healthcare ICT domains, I would like to invite you to participate in the validation of a novel Maturity Model for Healthcare Cloud Security System (MMHCSS). Should you accept, you will be expected to read through the attached information on the proposed maturity model and provide your feedback through the response document. All collected data relate to the appropriateness of the proposed model, rather than the level of maturity within your organisation. Any information you provide will be used in part fulfilment of PhD research at University of Plymouth, it will be kept anonymous. Your participation is voluntary and can be withdrawn should you choose to from the study.

The duration of providing your feedback to the questions will be 15-20 minutes. Once completed, please email your completed response document to opeoluwa.balogun@plymouth.ac.uk. Should you prefer to provide your response via an interview instead, please reply to this email indicating your preference. The audio from the interview will be recorded in that case. This study has received ethical approval by the University of Plymouth Faculty of Science and Engineering Research Ethics & Integrity Committee. Please do not hesitate to contact me through opeoluwa.balogun@plymouth.ac.uk should you have any questions about this study.

The diagram is a proposed Maturity Model for Healthcare Cloud Security (MMHCS), which consists of 4 maturity levels that apply to each of the following cloud security domains:

- Incident Response Management (IRM),
- Identity and Access Management (IAM),
- Enterprise Risk Management (ERM),
- Personnel Security (PeS),
- Physical Security (PhS)

Each domain includes a group of relevant objectives, which consist of processes and practices that could determine the maturity level in that domain.

Detailed description of M<sup>2</sup>HCS (Appendix A) was also included.

## **Appendix D - Survey Questions**



## PARTICIPANT'S CONSENT

Do you agree to participate in this study?

☐ Yes

☐ No

## Assessment Guidelines

Kindly complete the respondent's pre-assessment details

Kindly validate the model and each domain. Please refer to the related section and page in the document named 'Information'.

## RESPONDENT DETAILS

What best describes your current position? *Input response in letters (text)*

What is your background? *Academia, Healthcare, Cloud security, Cybersecurity, Input as apply*

What are your years of experience at this background? *Input the response in Numbers*

Do you have any experience in healthcare cloud/cyber-security? For how many years?

*Yes, No, 0 years - no experience, otherwise, input number of years*

What was the type of healthcare facility? *General/Acute-care Hospital, Community Health centre, District Hospital, Specialised Hospital, Teaching Hospital, Clinics, Private healthcare centre, Input as apply*

Have you participated previously in cloud/cyber-security maturity assessment?

Type of Assessment?

*Yes, No, Internal - Within an Organization, External - Outside an Organization*

**MATURITY MODEL VALIDATION (Refer to Section 1 page 2)** (Please provide responses with reasons)

Are the domains relevant for the assessment of maturity within an organisation?

- ☐ Strongly Agree      ☐ Agree      ☐ Disagree
- ☐ Strongly Disagree

Are the objectives relevant?

- ☐ Strongly Agree      ☐ Agree      ☐ Disagree
- ☐ Strongly Disagree

How feasible would it be to assess these objectives in practice?

- ☐ Strongly Agree      ☐ Agree      ☐ Disagree
- ☐ Strongly Disagree

Can the maturity model be practically used in healthcare industry?

- ☐ Strongly Agree      ☐ Agree      ☐ Disagree
- ☐ Strongly Disagree

## DOMAINS VALIDATION

### INCIDENT RESPONSE MANAGEMENT (Refer to Section 2A page 5)

Do you consider the controls appropriate for defining IRM levels?

- ☐ Strongly Agree      ☐ Agree      ☐ Disagree      ☐ Strongly Disagree

Which controls would you add or remove?

☐ Strongly Agree      ☐ Agree      ☐ Disagree      ☐ Strongly Disagree

Do you consider the descriptions correctly assigned to their respective maturity level?

☐ Strongly Agree      ☐ Agree      ☐ Disagree      ☐ Strongly Disagree

Do you consider the core control descriptions appropriate to attain a maturity level?

☐ Strongly Agree      ☐ Agree      ☐ Disagree      ☐ Strongly Disagree

## IDENTITY AND ACCESS MANAGEMENT (Refer to Section 2B page 9)

Do you consider the controls appropriate for defining IAM levels?

☐ Strongly Agree      ☐ Agree      ☐ Disagree      ☐ Strongly Disagree

Which controls would you add or remove?

☐ Strongly Agree      ☐ Agree      ☐ Disagree      ☐ Strongly Disagree

Do you consider the descriptions correctly assigned to their respective maturity level?

☐ Strongly Agree      ☐ Agree      ☐ Disagree      ☐ Strongly Disagree

Do you consider the core control descriptions appropriate to attain a maturity level?

☐ Strongly Agree      ☐ Agree      ☐ Disagree      ☐ Strongly Disagree

Do you consider the controls appropriate for defining ERM levels?

☐ Strongly Agree      ☐ Agree      ☐ Disagree      ☐ Strongly Disagree

Which controls would you add or remove?

☐ Strongly Agree      ☐ Agree      ☐ Disagree      ☐ Strongly Disagree

Do you consider the descriptions correctly assigned to their respective maturity level?



☐ Strongly Agree      ☐ Agree      ☐ Disagree      ☐ Strongly Disagree

Do you consider the core control descriptions appropriate to attain a maturity level?

☐ Strongly Agree      ☐ Agree      ☐ Disagree      ☐ Strongly Disagree

**PERSONNEL SECURITY (Refer to Section 2D page 17)**

Do you consider the controls appropriate for defining PeS levels?

☐ Strongly Agree      ☐ Agree      ☐ Disagree      ☐ Strongly Disagree

Which controls would you add or remove?

☐ Strongly Agree    ☐ Agree    ☐ Disagree    ☐ Strongly Disagree

Do you consider the descriptions correctly assigned to their respective maturity level?

☐ Strongly Agree    ☐ Agree    ☐ Disagree    ☐ Strongly Disagree

Do you consider the core control descriptions appropriate to attain a maturity level?

☐ Strongly Agree    ☐ Agree    ☐ Disagree    ☐ Strongly Disagree

**PHYSICAL SECURITY (Refer to Section 2E page 21)**

Do you consider the controls appropriate for defining PhS levels?

☐ Strongly Agree    ☐ Agree    ☐ Disagree    ☐ Strongly Disagree

Which controls would you add or remove?

☐ Strongly Agree    ☐ Agree    ☐ Disagree    ☐ Strongly Disagree

Do you consider the descriptions correctly assigned to their respective maturity level?

☐ Strongly Agree    ☐ Agree    ☐ Disagree    ☐ Strongly Disagree

Do you consider the core control descriptions appropriate to attain a maturity level?

☐ Strongly Agree    ☐ Agree    ☐ Disagree    ☐ Strongly Disagree

## **Appendix E - Interview Summary**

Dear [Interviewee Title & Surname]

### **LETTER OF INTRODUCTION & PURPOSE OF INTERVIEW**

I am Miss Opeoluwa Ore Balogun, a doctoral researcher of the School of Computing, Electronics and Mathematics at University of Plymouth. You have been approached to participate in this study as a result of your contribution to the [project name]. I would like to invite you to participate in a telephone interview that investigates the major access control challenges related to sharing and mobile rendering of cloud-based 3-dimensional medical radiological images in health care.

Your participation will involve a semi-structured interview over telephone. The expected duration is one (1) hour. Subject to your approval, the interview may be recorded and a transcript will be provided for your approval. All data will be kept anonymous and the interview recording will not be published or shared with other parties. Anonymised quotes and the analysis of anonymised collected data will form the basis for future research publications.

Please email [opeoluwa.balogun@plymouth.ac.uk](mailto:opeoluwa.balogun@plymouth.ac.uk) to confirm participation and to arrange an interview. At the same time, feel free to forward this invitation as appropriate to any other relevant parties that could contribute to the study. I sincerely hope that you will consider participating in this important effort to improve healthcare.

This study has received ethical approval by the [faculty name]. Should you have any questions or concerns about the way the interview has been conducted,

please contact [name, email address of approver]. Please do not hesitate to contact me should you have any questions about this study.

Sincerely,

[Name, title, and institution of the interviewer]

Telephone:

CSCAN profile URL:

## Appendix F - Interview Question Guide

### INTERVIEW QUESTIONS

#### SECTION A: PROFESSIONAL DEMOGRAPHICS

1. Cloud-based eHealth project

a. Have you been involved in a cloud-based eHealth project {yes/no}:

[ \_\_\_\_\_ ] (If your answer is no, go to question 2a)

If yes, please list the project(s) you have been involved with: <b>Project Name</b>	<b>Duration (month/year)</b>	<b>Deployment Models (private, public, community, hybrid<sup>1</sup>)</b>	<b>Archetypal Models (Software-as-a-Service, Platform-as-a-Service, Infrastructure-as-a-Service*)</b>

2. Cloud-based eHealth department

a. Have you worked in a unit involved in cloud-based eHealth {yes/no}:

[ \_\_\_\_\_ ] (If your answer is no, go to question 3).

---

<sup>1</sup><http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

- b. If yes, please list the department(s) you have worked in

Unit Name	Duration (month/year)	Deployment Models (private, public, community, hybrid*)	Archetypal Models (Software-as-a-Service, Platform-as-a-Service, Infrastructure-as-a- Service*)

#### **SECTION B: TECHNICAL PROBLEMS OF CLOUD-BASED eHEALTH**

- Cloud-based eHealth are mostly used for distribution of records within the same institution, used seldom for sharing, and very rarely for outsourcing for second or expert opinions and cross-border use cases. Based on your expertise, what security reasons would you consider to be limiting its use?
- How would you rate the following security and performance challenges of cloud-based eHealth, on a scale of 1-5, where 1 has least impact and 5 has very severe impact?



	Least Impact  1	Small Impact  2	Moderate Impact  3	Severe Impact  4	Very Severe Impact  5	No Opinion  N/A
Systems and data availability						
Lack of interoperability						
Access control and authentication						
Data integrity						
Network Security						
Application performance in the cloud						
Bandwidth consumption limitations						
Latency constraints – Response time and throughput						

- a. Could you provide more details to support your ratings?
- b. What is the most important in the limited adoption of cloud-based eHealth?

5. What do you consider the major access control (integrity and privacy) challenges of medical records faced in a cloud-based shared workflow?
6. To secure communication in a shared workflow, the records are encrypted before being shared using encryption or the hash function. Which do you consider or suggest being best suited in a shared eHealth workflow based in the cloud?
7. For secure, reliable and quick transmission over long distances and among different databases, very good access control mechanism(s) is/are required. Based on your expertise, which access control model(s) and policy(ies) is best suited for intra-organization, inter-organization and cross-border cloud-based teleradiology?
  - a. To verify access rights to a health record in the cloud, login/password, smartcard, single sign on, fingerprint and certificates can be used. Which do you consider most efficient without interrupting clinical workflow?
8. 'Exception access' in access control models increases the threat to patient privacy as it can be seen as a backdoor for misuse and also makes it infeasible to audit the access log for misuse. Do you consider 'exception access' a major technical security challenge?
  - a. 'Exception access' is provided mainly because of the dynamic nature of healthcare. What solutions do you suggest that could help to improve access control models to avoid the use of 'exception access'?

9. Healthcare is a sector with dynamic needs, yet the access control solutions offered are based on models with static nature. Would you consider this as a limitation of present access control solutions in healthcare?
10. What do you consider the major technical volume rendering challenges faced:
- a. when using a desktop?
  - b. When using mobile device (mobile phone, PDA, tablet)?
11. Apart from these technical security and performance challenges, are there any other major challenges/gaps in research especially concerning access control in cloud-based eHealth workflow?

### **SECTION C: MANAGERIAL PROBLEMS OF CLOUD-BASED eHEALTH**

12. How would you rate the following management challenges in the adoption of cloud-based eHealth, on a scale of 1-5, where 1 has least impact and 5 has very severe impact? :

	Least Impact	Small Impact	Moderate Impact	Severe Impact	Very Severe Impact	No Opinion
Lack of trust in data security and privacy controls						
Organizational inertia/cultural resistance						
Manageability - vendor lock-in						
Legal regulations						
Standardisation, compliance and trust						

a. Could you provide more details to support your ratings?

13. RxEye Cloud is one of the various cloud-based teleradiology platforms that is used in Europe, implementations mainly occurs in member states with a high concentration of networked Picture Archiving and Communication Systems (PACS), whilst usage of commercial teleradiology services in Europe is relatively limited, as language seems to be a limiting factor for further deployment of services and the demand for a Pan-European legislation, price regulation and quality assurance framework.

- a. What do you consider to be the 'things' that could have been done differently to enhance adoption of cloud-based systems in eHealth?
- b. What is/are future directions for cloud-based eHealth systems?
- c. Kindly add any other information you consider very important to this survey.

Assuming you had a budget to assign for the different factors influencing the adoption of cloud-based eHealth, including technical security, performance, and management challenges, how would you apportion it between them? Assign the percentage you would consider appropriate for each:	Percentage	Justification
Technical Security		
Performance		
Management		

## Bibliography

- AbuKhoussa, E., Mohamed, N. and Al-Jaroodi, J. (2012) 'e-Health Cloud: Opportunities and Challenges', *Future Internet*. Molecular Diversity Preservation International, 4(4), pp. 621–645. doi: 10.3390/fi4030621.
- Adams, A. and Sasse, M. A. (1999) 'Users are not the enemy', *Communications of the ACM*. ACM, 42(12), pp. 40–46. doi: 10.1145/322796.322806.
- Akinsanya, O. O., Papadaki, M. and Sun, L. (2019a) 'Current Cyber Security Maturity Models: How Effective in Healthcare Cloud?', in Udo Bleimann et al. (eds) *5th Collaborative European Research Conference (CERC 2019)*. Darmstadt, Germany: CEUR Workshop (CEUR-WS.org), pp. 211–222. Available at: <http://ceur-ws.org/Vol-2348/paper16.pdf> (Accessed: 6 June 2019).
- Akinsanya, O. O., Papadaki, M. and Sun, L. (2019b) 'Factors Limiting the Adoption of Cloud Computing in Teleradiology', *International Journal for Information Security Research (IJISR)*, 9(2), pp. 854–861. doi: 10.20533/IJISR.2042.4639.2019.0098.
- Almorsy, M., Grundy, J. and Müller, I. (2010) 'An Analysis of the Cloud Computing Security Problem', in *the Asia Pacific Cloud Workshop, Co-located with Asia Pacific Software Engineering Conference (APSEC '10)*. Sydney, Australia. Available at: <http://arxiv.org/abs/1609.01107> (Accessed: 3 July 2019).
- Ammenwerth, E. et al. (2003) 'Medical Informatics and the Quality of Health: New Approaches to Support Patient Care', *International Medical Informatics Association (IMIA)*, p. 185. Available at: <https://pdfs.semanticscholar.org/a34d/59e43f61fd02bcb96b0029cb0e6ae0b25f2c.pdf> (Accessed: 29 June 2017).

Ancker, J. S. *et al.* (2013) 'Consumer experience with and attitudes toward health information technology: a nationwide survey.', *Journal of the American Medical Informatics Association : JAMIA*. American Medical Informatics Association, 20(1), pp. 152–6. doi: 10.1136/amiajnl-2012-001062.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2012). Brussels. Available at: [http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29\\_press\\_material/2012/20120701\\_wp\\_196\\_cloud\\_computing\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2012/20120701_wp_196_cloud_computing_en.pdf) (Accessed: 30 June 2017).

Athena (2017) *MODEL-DRIVEN EUROPEAN PAEDIATRIC REPOSITORY*. Available at: <https://www.athena-innovation.gr/el/ek-athina/projects/model-driven-european-paediatric-repository> (Accessed: 29 April 2019).

Axelrod, C. W. (2008) 'Accounting for Value and Uncertainty in Security Metrics', *Information Systems Control Journal*, 6. Available at: <https://www.researchgate.net/publication/268059625> (Accessed: 29 May 2019).

Azhar, M. *et al.* (2014) 'Secured Health Monitoring System in Mobile Cloud Computing', *International Journal of Computer Trends and Technology*, 13(3). Available at: <http://www.ijctjournal.org> (Accessed: 2 April 2019).

Balogun, O. O. and Papadaki, M. (2018) 'Organizational Factors Influencing Medical Data Sharing in Cloud', in *Infonomics Society*. Cambridge, London: Internet Technology and Secured Transactions (ICITST-2018), pp. 184–187. doi: 10.2053//ICITST.WorldCIS.WCST.WCICSS.2018.0029.

Barabanov, R., Kowalski, S. and Yngström, L. (2012) *Information Security Metrics: Research Directions*. Available at: <http://www.diva->

- portal.org/smash/get/diva2:469569/FULLTEXT01.pdf (Accessed: 21 May 2019).
- Bath, P. A. (2008) 'Health Informatics: current issues and challenges', *Journal of Information Science*, 34(4), pp. 501–518. Available at: [http://eprints.whiterose.ac.uk/78563/8/WRRO\\_78563.pdf](http://eprints.whiterose.ac.uk/78563/8/WRRO_78563.pdf) (Accessed: 1 July 2017).
- Becker, J., Knackstedt, R. and Pöppelbuß, J. (2009) 'Developing Maturity Models for IT Management', *Business & Information Systems Engineering*. SP Gabler Verlag, 1(3), pp. 213–222. doi: 10.1007/s12599-009-0044-5.
- Beres, Y. *et al.* (2009) 'Using security metrics coupled with predictive modeling and simulation to assess security processes', in *3rd International Symposium on Empirical Software Engineering and Measurement*. Lake Buena Vista, Florida: IEEE, pp. 564–573. doi: 10.1109/ESEM.2009.5314213.
- Bevan, N. (2009) *International Standards for Usability Should Be More Widely Used*, *Journal of Usability Studies*. Available at: [http://uxpajournal.org/wp-content/uploads/sites/8/pdf/JUS\\_Bevan\\_May2009.pdf](http://uxpajournal.org/wp-content/uploads/sites/8/pdf/JUS_Bevan_May2009.pdf) (Accessed: 18 July 2019).
- Bevan, N., Carter, J. and Harker, S. (2015) 'ISO 9241-11 Revised: What Have We Learnt About Usability Since 1998?', *Kurosu M. (eds) Human-Computer Interaction: Design and Evaluation.HCI 2015. Lecture Notes in Computer Science*. Springer, Cham, 9169, pp. 143–151. doi: 10.1007/978-3-319-20901-2\_13.
- Bevan, N. and Nigel (2006) 'Practical issues in usability measurement', *interactions*. ACM, 13(6), p. 42. doi: 10.1145/1167948.1167976.
- Bishop, M. (2003) 'What is computer security?', *IEEE Security & Privacy*



*Magazine*, 1(1), pp. 67–69. doi: 10.1109/MSECP.2003.1176998.

Bourdon, R. (2019) *WampServer, a Windows web development environment, WampServer*. Available at: <http://www.wampserver.com/en/> (Accessed: 18 July 2019).

Bruin, D. *et al.* (2005) 'Understanding the Main Phases of Developing a Maturity Assessment Model', in *Australasian Conference on Information Systems (ACIS)*. New South Wales, Sydney. Available at: <https://eprints.qut.edu.au/25152/> (Accessed: 21 May 2019).

De Bruin, T. *et al.* (2005) 'Understanding the Main Phases of Developing a Maturity Assessment Model', in Campbell, B., Underwood, J., and Bunker, D. (eds) *Australasian Conference on Information Systems (ACIS)*. Australia, New South Wales, Sydney. Available at: <https://eprints.qut.edu.au/25152/> (Accessed: 22 May 2019).

Carvalho, J. V. *et al.* (2017) 'Development methodology of the HISMM Maturity Model', in *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE, pp. 1–7. doi: 10.23919/CISTI.2017.7975998.

Catteddu, D. and Hogben, G. (2009) *Cloud Computing - Benefits, Risks and Recommendation for Information Security*. Available at: <https://www.pdpjournals.com/docs/88049.pdf> (Accessed: 9 October 2018).

Chew, Elizabeth *et al.* (2008) *Performance Measurement Guide for Information Security: NIST Special Publication 800-55 Revision 1*. Gaithersburg, MD. doi: 10.6028/NIST.SP.800-55r1.

Chew, E *et al.* (2008) *Performance measurement guide for information security*.

Gaithersburg, MD. doi: 10.6028/NIST.SP.800-55r1.

Christopher, J. D. *et al.* (2014) *ELECTRICITY SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)*. Available at: <https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf>.

*CIS Security Metrics-Quick Start Guide v1.0.0* (2010). Available at: [http://www.itsecure.hu/library/image/CIS\\_Security\\_Metrics-Quick\\_Start\\_Guide\\_v1.0.0.pdf](http://www.itsecure.hu/library/image/CIS_Security_Metrics-Quick_Start_Guide_v1.0.0.pdf) (Accessed: 18 February 2019).

Cloud Standards Customer Council (2015) *Practical Guide to Cloud Service Agreements Version 2.0*.

Conwell, L. C., Rosemary, E. and Marcia, A. S. (2000) 'Capability maturity models support of modeling and simulation verification, validation, and accreditation', in *Proceedings of the 32nd conference on Winter simulation*. Society for Computer Simulation International, pp. 819–828. Available at: <https://dl.acm.org/citation.cfm?id=510496> (Accessed: 22 May 2019).

CSA (2011) *Security Guidance for Critical Areas of Focus in Cloud Computing v3.0*. Available at: <http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>.

CSA (2017) *Introduction to Cloud Control Matrix (CCM)*. Available at: <https://cloudsecurityalliance.org/> (Accessed: 17 July 2019).

Das, A. K. *et al.* (2018) 'Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment', *IEEE Journal of Biomedical and Health Informatics*, 22(4), pp. 1310–1322. doi: 10.1109/JBHI.2017.2753464.

Donabedian, A. (1988) 'The Quality of Care', *JAMA*. American Medical

Association, 260(12), p. 1743. doi: 10.1001/jama.1988.03410120089033.

Duff, A. (1996) 'The literature search: a library-based model for information skills instruction', *Library Review*. MCB UP Ltd, 45(4), pp. 14–18. doi: 10.1108/00242539610115263.

Duncan, B. and Whittington, M. (2014) 'Compliance with standards, assurance and audit: does this equal security?', in *Proceedings of the 7th International Conference on Security of Information and Networks - SIN '14*. New York: ACM Press, pp. 77–84. doi: 10.1145/2659651.2659711.

eHealth Network (2015) *Refined eHealth European Interoperability Framework (ReEIF)*. Brussels.

Elmaallam, M. and Kriouile, A. (2013) 'Toward a Maturity Model Development Process for Information Systems (MMDePSI)', *International Journal of Computer Science Issues (IJCSI)*, 10(3), pp. 118–125. Available at: [www.IJCSI.org](http://www.IJCSI.org) (Accessed: 21 May 2019).

ESR (2012) *ESR response to consultation on the eHealth Action Plan (eHAP)*. Available at: [http://www.myesr.org/sites/default/files/eHealth\\_Action\\_plan\\_ESR\\_Response\\_final\\_0.pdf](http://www.myesr.org/sites/default/files/eHealth_Action_plan_ESR_Response_final_0.pdf) (Accessed: 30 June 2017).

Eysenbach, G. (2001) 'What is e-health?', *Journal of medical Internet research*. Journal of Medical Internet Research, 3(2), p. E20. doi: 10.2196/jmir.3.2.e20.

Fitzgerald, G., Piris, L. and Serrano, A. (2008) 'Identification of Benefits and Barriers for the Adoption of E-Health Information Systems Using a Socio-Technical Approach', in *Proceedings of the ITI 2008 30th Int. Conf. on Information*

*Technology Interfaces*. Croatia. Available at: <http://ai2-s2-pdfs.s3.amazonaws.com/5e8b/28e4c008651fda50e361c78a3a88fc108950.pdf>  
(Accessed: 30 June 2017).

Flanagan, P. T. *et al.* (2012) 'Using the Internet for Image Transfer in a Regional Trauma Network: Effect on CT Repeat Rate, Cost, and Radiation Exposure', *Journal of the American College of Radiology*, 9(9), pp. 648–656. doi: 10.1016/j.jacr.2012.04.014.

Flanders, A. E. (2009) 'Medical Image and Data Sharing: Are We There Yet?', *RadioGraphics*, 29(5), pp. 1247–1251. doi: 10.1148/rq.295095151.

Freund, J. *et al.* (2006) 'Health-e-child: an integrated biomedical platform for grid-based paediatric applications.', *Studies in health technology and informatics*, 120, pp. 259–70. Available at: <http://www.ncbi.nlm.nih.gov/pubmed/16823144>  
(Accessed: 29 April 2019).

Gaylin, D. S. *et al.* (2011) 'Public attitudes about health information technology, and its relationship to health care quality, costs, and privacy.', *Health services research*. Health Research & Educational Trust, 46(3), pp. 920–38. doi: 10.1111/j.1475-6773.2010.01233.x.

Gill, L. and White, L. (2009) 'A critical review of patient satisfaction', *Leadership in Health Services*. Emerald Group Publishing Limited, 22(1), pp. 8–19. doi: 10.1108/17511870910927994.

Giokas, D., Sekhon, H., Mestre, A., Geffen, M., Nouri, H. and Twoekowski, K. (2015) *A Discussion Paper for Health Information Network (HIN) Capability Maturity Model*. Available at:

<https://www.colleaga.org/sites/default/files/attachments/hin-discussion-paper->

maturity-model-en.pdf.

Giokas, D., Sekhon, H., Mestre, A., Geffen, M., Nouri, H. and Tworkowski, K. (2015) *A White Paper - Health Information Network (HIN) Leading Practices*. Available at: <https://www.infoway-inforoute.ca/en/component/edocman/2836-health-information-network-hin-leading-practices/view-document?Itemid=0>.

Glazer, G. M. and Ruiz-Wibbelsmann, J. A. (2011) 'The Invisible Radiologist', *Radiology*. Radiological Society of North America, Inc., 258(1), pp. 18–22. doi: 10.1148/radiol.10101447.

Graham, C. (2017) 'NHS cyber attack: Everything you need to know about "biggest ransomware" offensive in history', *The Telegraph*, 20 May. Available at: <http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/> (Accessed: 30 June 2017).

Gunamalai, C. and Sivasubramanian, S. (2015) 'A NOVEL METHOD OF SECURITY AND PRIVACY FOR PERSONAL MEDICAL RECORD AND DICOM IMAGES IN CLOUD COMPUTING', 10(10). Available at: [www.arpnjournals.com](http://www.arpnjournals.com) (Accessed: 2 April 2019).

Gupta, V. (2015) *Cloud Computing in Healthcare*, Cisco Knowledge Network. Available at: [https://www.cisco.com/c/en\\_in/about/knowledge-network/cloud-computing.html](https://www.cisco.com/c/en_in/about/knowledge-network/cloud-computing.html) (Accessed: 4 July 2019).

Haeberlen, T. and Dupre, L. (2012) *Cloud Computing Benefits, risks and recommendations for information security*. Available at: <http://www.enisa.europa.eu> (Accessed: 3 July 2019).

Hashizume, K. *et al.* (2013) 'An analysis of security issues for cloud computing',

*Journal of Internet Services and Applications, a SpringerOpen Journal*, 4(5), p. 13. doi: 10.1186/1869-0238-4-5.

Haufe, K., Dzombeta, S. and Brandis, K. (2014) 'Proposal for a security management in cloud computing for health care.', *TheScientificWorldJournal*. Hindawi Limited, 2014, p. 146970. doi: 10.1155/2014/146970.

Herrmann, D. S. (2007) *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI*. 1st edn. Auerbach Publications, London.

Hevner, R. A. *et al.* (2004) 'Design science in information systems research', *MIS Quarterly*. Society for Management Information Systems, 28(1), pp. 75–105. Available at: <https://dl.acm.org/citation.cfm?id=2017217> (Accessed: 9 October 2018).

Hill, J. W. and Powell, P. (2009) 'The national healthcare crisis: Is eHealth a key solution?', *Business Horizons*, 52, pp. 265–277. doi: 10.1016/j.bushor.2009.01.006.

HIMSS (2017) *CS0405 - Top 10 Cloud Security Concerns*. Chicago. Available at: <https://www.himss.org/library/healthcare-privacy-security/cloud-security/toolkit> (Accessed: 17 July 2019).

Huang, H. K. *et al.* (2005) *Data Grid for Large-Scale Medical Image Archive and Analysis*, *MM'05*. Singapore. Available at: <http://www.ipilab.org/Research/DataGrid/p1005-huang.pdf> (Accessed: 28 June 2017).

*Impact of Cloud Computing on Healthcare Version 2.0* (2017). Available at:

<http://www.cloud-council.org/deliverables/CSCC-Impact-of-Cloud-Computing-on-Healthcare.pdf> (Accessed: 29 June 2017).

*International Statistical Classification of Diseases and Related Health Problems ICD-10* (2010). Available at: [http://www.who.int/about/licensing/copyright\\_form](http://www.who.int/about/licensing/copyright_form) (Accessed: 30 June 2017).

Ionasec R., Suehling M. and Comaniciu D. (2010) *Sim-e-Child: Grid-Enabled Platform for Simulations in Paediatric Cardiology Toward the Personalized Virtual Child Heart, Virtual Physiological Human Network of Excellence (VPH NoE)*. Available at: <http://www.sim-e-child.org/> (Accessed: 29 April 2019).

Jafari, S. *et al.* (2010) 'Security Metrics for e-Healthcare Information Systems: A Domain Specific Metrics Approach', *International Journal of Digital Society (IJDS)*, 1(4). Available at: <https://pdfs.semanticscholar.org/f509/c235535cd2f9af4084c3a729bbbc7123e789.pdf>.

Jansen, W. (2009) *Directions in Security Metrics Research (NISTIR 7564)*. Gaithersburg, USA. doi: 10.6028/NIST.IR.7564.

Jansen, W. and Grance, T. (2011) *Guidelines on security and privacy in public cloud computing*. Gaithersburg, MD. doi: 10.6028/NIST.SP.800-144.

Jaquith, A. (2007) *Security metrics: replacing fear, uncertainty, and doubt*. Addison-Wesley.

Josh, M. and DePierro, D. (2018) *The Financial Services Sector Cybersecurity Profile (Profile), v1.0-An Overview and User Guide*. Available at: [https://fsscc.org/files/galleries/Financial\\_Services\\_Sector\\_Cybersecurity\\_Profile](https://fsscc.org/files/galleries/Financial_Services_Sector_Cybersecurity_Profile)

\_Overview\_and\_User\_Guide\_2018-10-25.pdf.

Kelly, J., Sadeghieh, T. and Adeli, K. (2014) 'Peer Review in Scientific Publications: Benefits, Critiques, & A Survival Guide.', *The Journal of the International Federation of Clinical Chemistry and Laboratory Medicine (EJIFCC)*. International Federation of Clinical Chemistry and Laboratory Medicine, 25(3), pp. 227–43. Available at: <http://www.ncbi.nlm.nih.gov/pubmed/27683470> (Accessed: 19 July 2019).

Kert, M., Markatos, E. and Preneel, B. (2015) *State of the art of secure ICT landscape*. Available at: <https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/state-of-the-art-of-the-secure-ict-landscape/view> (Accessed: 6 March 2019).

Khalil, I. M., Khreishah, A. and Azeem, M. (2014) 'Cloud Computing Security: A Survey', *Computers*. Multidisciplinary Digital Publishing Institute, 3(1), pp. 1–35. doi: 10.3390/computers3010001.

Khan, F. A. *et al.* (2014) 'A Cloud-based Healthcare Framework for Security and Patients' Data Privacy Using Wireless Body Area Networks', *Procedia Computer Science*. Elsevier, 34, pp. 511–517. doi: 10.1016/J.PROCS.2014.07.058.

Koo, C. J. and Kim, J. (2015) 'Decision Making for the Adoption of Cloud Computing for Sensor Data: From the Viewpoint of Industrial Security', *International Journal of Distributed Sensor Networks*. SAGE PublicationsSage UK: London, England, 11(9), p. 581563. doi: 10.1155/2015/581563.

Kuo, A. M.-H. (2011) 'Opportunities and challenges of cloud computing to improve health care services.', *Journal of medical Internet research*. JMIR Publications Inc., 13(3), p. e67. doi: 10.2196/jmir.1867.



Lacity, M. C. and Willcocks, L. (2012) *Advanced outsourcing practice : rethinking ITO, BPO and cloud services*.

Langkos, S. (2014) *CHAPTER 3 - RESEARCH METHODOLOGY: Data collection method and Research tools*. University of Derby. Available at: [https://www.academia.edu/10092020/CHAPTER\\_3\\_-\\_RESEARCH\\_METHODOLOGY\\_Data\\_collection\\_method\\_and\\_Research\\_tools](https://www.academia.edu/10092020/CHAPTER_3_-_RESEARCH_METHODOLOGY_Data_collection_method_and_Research_tools) (Accessed: 29 June 2017).

Le, N. T. and Hoang, D. B. (2017) 'Capability Maturity Model and Metrics Framework for Cyber Cloud Security', in *Special Issue on Communication, Computing, and Networking in Cyber-Physical Systems*. Universitatea de Vest din Timisoara, pp. 277–290. doi: 10.12694/scpe.v18i4.1329.

Lian, J.-W., Yen, D. C. and Wang, Y.-T. (2014) 'An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital', *International Journal of Information Management*. Pergamon, 34(1), pp. 28–36. doi: 10.1016/J.IJINFOMGT.2013.09.004.

Lo, O. *et al.* (2013) *Conducting Performance Evaluation of an e-Health Platform*. Ediburgh Napier University. doi: 10.4018/978-1-4666-4062-7.ch016.

Lounis, A. (2014) *Security in cloud computing*. Universit'e de Technologie de Compi'egne. Available at: <https://tel.archives-ouvertes.fr/tel-01293631> (Accessed: 29 June 2017).

Magrabi, F. *et al.* (2015) 'Clinical safety of England's national programme for IT: A retrospective analysis of all reported safety events 2005 to 2011', *International Journal of Medical Informatics*, 84(3), pp. 198–206. doi: 10.1016/j.ijmedinf.2014.12.003.

- March, S. T. and Smith, G. F. (1995) 'Design and natural science research on information technology', *Decision Support Systems*. North-Holland, 15(4), pp. 251–266. doi: 10.1016/0167-9236(94)00041-2.
- Masud, M. and Hossain, M. S. (2018) 'Secure data-exchange protocol in a cloud-based collaborative health care environment', *Multimedia Tools and Applications*. Kluwer Academic Publishers, 77(9), pp. 11121–11135. doi: 10.1007/s11042-017-5294-5.
- McHugh, J., Fithen, W. L. and Arbaugh, W. A. (2000) 'Windows of vulnerability: a case study analysis', *Computer*, 33(12), pp. 52–59. doi: 10.1109/2.889093.
- Mehraeen, E. *et al.* (2016) 'Security Challenges in Healthcare Cloud Computing: A Systematic Review', *Global Journal of Health Science*, 9(3), p. 157. doi: 10.5539/gjhs.v9n3p157.
- Mell, P. M. and Grance, T. (2011) *The NIST definition of cloud computing*. Gaithersburg, MD. doi: 10.6028/NIST.SP.800-145.
- Mendelson, D. S. *et al.* (2008) 'Image Exchange: IHE and the Evolution of Image Sharing', *RadioGraphics*. Radiological Society of North America, 28(7), pp. 1817–1833. doi: 10.1148/rg.287085174.
- Mendelson, D. S., Erickson, B. J. and Choy, G. (2014) 'Image sharing: evolving solutions in the age of interoperability.', *Journal of the American College of Radiology: JACR*. NIH Public Access, 11(12 Pt B), pp. 1260–9. doi: 10.1016/j.jacr.2014.09.013.
- Mettler, T. and Rohner, P. (2009) 'Situational maturity models as instrumental artifacts for organizational design', in *Proceedings of the 4th International*

*Conference on Design Science Research in Information Systems and Technology - DESRIST '09*. New York, New York, USA: ACM Press, p. 1. doi: 10.1145/1555619.1555649.

Mimoso, M. (2009) *Number-driven risk metrics 'fundamentally broken'*, *Tech Target*. Available at: <https://searchsecurity.techtarget.com/news/1350658/Number-driven-risk-metrics-fundamentally-broken> (Accessed: 29 May 2019).

Moen, A. *et al.* (2013) 'eHealth in Europe – Status and Challenges', *Yearbook of Medical Informatics*, 22(01), pp. 59–63. doi: 10.1055/s-0038-1638833.

Monrad, I. H. A. (2007) *The Organizational Challenge for Health Care from Telemedicine and eHealth (PDF Download Available)*. The Work Research Institute. Available at: [https://www.researchgate.net/publication/262395014\\_The\\_Organizational\\_Challenge\\_for\\_Health\\_Care\\_from\\_Telemedicine\\_and\\_eHealth](https://www.researchgate.net/publication/262395014_The_Organizational_Challenge_for_Health_Care_from_Telemedicine_and_eHealth) (Accessed: 29 June 2017).

De Moor, G. *et al.* (2014) 'Opportunities for Clinical Research in European Hospitals: The EHR4CR Platform', *Health Management*, 14(3). Available at: <https://healthmanagement.org/c/healthmanagement/issuearticle/opportunities-for-clinical-research-in-european-hospitals-the-ehr4cr-platform> (Accessed: 30 April 2019).

De Moor, G. *et al.* (2015) 'Using electronic health records for clinical research: The case of the EHR4CR project', *Journal of Biomedical Informatics*, 53, pp. 162–173. doi: 10.1016/j.jbi.2014.10.006.

Moreno-Conde, J. *et al.* (2015) 'Contextual cloud-based service oriented

242

architecture for clinical workflow', *Studies in health technology and informatics*, 210, pp. 592–596. doi: 10.3233/978-1-61499-512-8-592.

NHS (2011a) *NHS Infrastructure Maturity Model (NIMM)*, *The National Archives*. Available at: <https://webarchive.nationalarchives.gov.uk/20110503144044/http://www.connectingforhealth.nhs.uk/systemsandservices/nimm> (Accessed: 1 April 2019).

NHS (2011b) *The UK Edition of SNOMED CT as the Fundamental Standard for Clinical Terminology within the NHS in England Requirement and Draft for a Fundamental Information Standard*. Available at: <http://webarchive.nationalarchives.gov.uk/+/http://www.isb.nhs.uk/documents/isb-0034/amd-26-2006/0034262006draftsub.pdf> (Accessed: 30 June 2017).

NHS Digital (2018) *Data Security Standard Overall Guide*. Available at: <https://www.dsptoolkit.nhs.uk/Help/Attachment/24> (Accessed: 16 July 2019).

NHS England, HSCIC, South, C. and W. C. S. U. (2015) *Interoperability Handbook*. Available at: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/474444/interoperability-handbook.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/474444/interoperability-handbook.pdf) (Accessed: 2 December 2019).

NHS England, S. S. and T. (2014) *General Practice IT Infrastructure Specification*. Available at: [www.england.nhs.uk/ourwork/tsd/sst/it-pc/](http://www.england.nhs.uk/ourwork/tsd/sst/it-pc/).

NIST (2017) *Framework for Improving Critical Infrastructure Cybersecurity*. Available at: <https://www.nist.gov/sites/default/files/documents/draft-cybersecurity-framework-v1.1-with-markup1.pdf> (Accessed: 15 July 2019).

Okoli, C. and Schabram, K. (2010) 'A Guide to Conducting a Systematic

Literature Review of Information Systems Research', *Sprouts: Working Papers on Information Systems*, 10(26). Available at: <https://pdfs.semanticscholar.org/31dc/753345d5230e421ea817dd7dcdd352e87ea2.pdf>.

Parker, P. (2018) *Interview: Why the NHS is struggling to move to the Cloud?, Building Better Healthcare*. Available at: [https://www.buildingbetterhealthcare.co.uk/news/article\\_page/Interview\\_Why\\_the\\_NHS\\_is\\_struggling\\_to\\_move\\_to\\_the\\_Cloud/141118](https://www.buildingbetterhealthcare.co.uk/news/article_page/Interview_Why_the_NHS_is_struggling_to_move_to_the_Cloud/141118) (Accessed: 4 July 2019).

Parodi, O. (2016) *E-health: 3D, a new ally for coronary arteries with SMARTool, Research Italy*. Available at: <https://www.researchitaly.it/en/projects/e-health-3d-a-new-ally-for-coronary-arteries-with-smartool/#null> (Accessed: 29 April 2019).

Pasche, E. *et al.* (2016) *Model Driven Paediatric European Digital Repository*. Available at: <http://www.md-paedegree.eu/wp-content/uploads/2016/04/MD-Paedegree-D17.4-Test-on-the-prototype-for-the-case-and-ontology-based-retrieval-service-.pdf> (Accessed: 29 April 2019).

Payne, S. C. (2007) *A Guide to Security Metrics*. Available at: <https://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55>.

Peffer, K. *et al.* (2008) 'A Design Science Research Methodology for Information Systems Research', *Journal of Management Information Systems*, 24(8), pp. 45–78. Available at: <http://www.tuunanen.fi>. (Accessed: 3 July 2019).

Philbin, J., Prior, F. and Nagy, P. (2011) 'Will the next generation of PACS be sitting on a cloud?', *Journal of digital imaging*. Springer, 24(2), pp. 179–83. doi: 10.1007/s10278-010-9331-4.

- Rahman, S. M. M. *et al.* (2016) 'Privacy preserving secure data exchange in mobile P2P cloud healthcare environment', *Peer-to-Peer Networking and Applications*. Springer US, 9(5), pp. 894–909. doi: 10.1007/s12083-015-0334-2.
- Ranschaert, E. R. and Binkhuysen, F. H. B. (2013) 'European Teleradiology now and in the future: results of an online survey.', *Insights into imaging*. Springer, 4(1), pp. 93–102. doi: 10.1007/s13244-012-0210-z.
- Rao, R. V. and Selvamani, K. (2015) 'Data Security Challenges and Its Solutions in Cloud Computing', *Procedia Computer Science*. Elsevier, 48, pp. 204–209. doi: 10.1016/J.PROCS.2015.04.171.
- Reddy, V. K. (2015) *Security Architecture of Cloud Computing*. Available at: <https://www.researchgate.net/publication/299572565> (Accessed: 2 April 2019).
- Robert, G. *et al.* (2009) 'Organisational factors influencing technology adoption and assimilation in the NHS: a systematic literature review James Clerk Maxwell Building'. Available at: [http://www.netscc.ac.uk/hsdr/files/project/SDO\\_FR\\_08-1819-223\\_V01.pdf](http://www.netscc.ac.uk/hsdr/files/project/SDO_FR_08-1819-223_V01.pdf) (Accessed: 16 May 2018).
- Rocchiccioli, S. *et al.* (2017) *SMARTool – Simulation Modeling of coronary ARTery disease: a tool for clinical decision support*. Available at: <http://www.smartool.eu/> (Accessed: 29 April 2019).
- Rodrigues, J. *et al.* (2013) 'Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems', *Journal of Medical Internet Research*, 15(8), p. e186. doi: 10.2196/jmir.2494.
- Saevanee, H. *et al.* (2015) 'Continuous user authentication using multi-modal biometrics', *Computers & Security*. Elsevier Advanced Technology, 53, pp. 234–

246. doi: 10.1016/J.COSE.2015.06.001.

Safa, N. S. *et al.* (2015) 'Information security conscious care behaviour formation in organizations', *Computers & Security*. Elsevier Advanced Technology, 53, pp. 65–78. doi: 10.1016/J.COSE.2015.05.012.

Sakellarios, A. I. *et al.* (2017) 'SMARTool: A tool for clinical decision support for the management of patients with coronary artery disease based on modeling of atherosclerotic plaque process', in *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. IEEE, pp. 96–99. doi: 10.1109/EMBC.2017.8036771.

Sanson-Fisher, R. W. (2014) 'Diffusion of innovation theory for clinical change', *Medical Journal of Australia*. John Wiley & Sons, Ltd, 180, pp. S55–S56. doi: 10.5694/J.1326-5377.2004.TB05947.X.

Savage, M. (2009) 'NHS "loses" thousands of medical records', *The Independent*, 24 May. Available at: <http://www.independent.co.uk/news/uk/politics/nhs-loses-thousands-of-medical-records-1690398.html> (Accessed: 30 June 2017).

Savvides, A. (2009) *NHS Infrastructure Maturity Model BCS/ASSIST Presentation*. Available at: <http://nww.connectingforhealth.nhs.uk/pspg/>.

Schneier, B. (2000) *Secrets and lies : digital security in a networked world*. New York: John Wiley. Available at: [https://primo.plymouth.ac.uk/primo-explore/fulldisplay?docid=44PLY\\_ALMA\\_DS2139942790001281&context=L&vid=VU\\_PLY&lang=en\\_US&adaptor=LocalSearchEngine&tab=local&query=any,contains,B.Schneier, Secrets and lies: digital security in a](https://primo.plymouth.ac.uk/primo-explore/fulldisplay?docid=44PLY_ALMA_DS2139942790001281&context=L&vid=VU_PLY&lang=en_US&adaptor=LocalSearchEngine&tab=local&query=any,contains,B.Schneier,Secrets+and+lies:digital+security+in+a) (Accessed: 18 February 2019).

Schneier, B. (2004) *Secrets and lies : digital security in a networked world*. John Wiley & Sons. Available at: <https://www.wiley.com/en-gb/Secrets+and+Lies:+Digital+Security+in+a+Networked+World-p-9780471453802>.

Scott, J. and Harder, R. (2017) *Network Security Policy*. Available at: <https://www.plymouthhospitals.nhs.uk/trust-policies> (Accessed: 23 June 2019).

'Security for Cloud Computing Ten Steps to Ensure Success Version 2.0' (2015) *Cloud Standards Customer Council*. Available at: <http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf> (Accessed: 29 June 2017).

Shaw, R. (2018) *NHS Digital publishes guidance on data off-shoring and cloud computing for health and social care, NHS Digital*. Available at: <https://digital.nhs.uk/news-and-events/latest-news/nhs-digital-publishes-guidance-on-data-off-shoring-and-cloud-computing-for-health-and-social-care> (Accessed: 18 July 2019).

Sheng, S. *et al.* (2006) 'Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software', in *Proceedings of the Second Symposium on Usable Privacy and Security, SOUPS '06*. Pittsburgh, PA. Available at: [https://cups.cs.cmu.edu/soups/2006/posters/sheng-poster\\_abstract.pdf](https://cups.cs.cmu.edu/soups/2006/posters/sheng-poster_abstract.pdf) (Accessed: 10 July 2019).

Shin, S., Kobara, K. and Imai, H. (2012) 'A secure public cloud storage system', in *Internet Technology and Secured Transactions (ICITST)*. Abu Dhabi, UAE: IEEE. Available at: <http://ieeexplore.ieee.org/document/6148361/> (Accessed: 29 June 2017).



Shini, S. G., Thomas, T. and Chithraranjan, K. (2012) 'Cloud Based Medical Image Exchange-Security Challenges', *Procedia Engineering*, 38, pp. 3454–3461. doi: 10.1016/j.proeng.2012.06.399.

Solove, D. J. (2013) 'HIPAA Turns 10: Analyzing the Past, Present, and Future Impact', *84 Journal of AHIMA* 22-28 (2013); *GWU Legal Studies Research Paper No. 2013-75*; *GWU Law School Public Law Research Paper No. 2013-75*, pp. 22–28. Available at: [http://scholarship.law.gwu.edu/faculty\\_publications](http://scholarship.law.gwu.edu/faculty_publications) (Accessed: 3 July 2019).

Sonehara, N., Echizen, I. and Wohlgemuth, S. (2011) 'Isolation in Cloud Computing and Privacy-Enhancing Technologies', *Business & Information Systems Engineering*. SP Gabler Verlag, 3(3), pp. 155–162. doi: 10.1007/s12599-011-0160-x.

Spruit, M. and Röling, M. (2014) 'ISFAM: THE INFORMATION SECURITY FOCUS AREA MATURITY MODEL', in *European Conference on Information Systems (ECIS)*. Tel Aviv: AIS Electronic Library (AISeL), p. 16. Available at: <http://aisel.aisnet.org/ecis2014><http://aisel.aisnet.org/ecis2014/proceedings/track14/6>.

Staggers, N. *et al.* (2011) *Promoting Usability in Health Organizations: Initial Steps and Progress Toward a Healthcare Usability Maturity Model*. Available at: <https://www.himss.org/sites/himssorg/files/2013-HIMSS-Usability-Maturity-Model.pdf> (Accessed: 11 July 2019).

Stroetmann, K. A. *et al.* (2011) *European countries on their journey towards national eHealth infrastructures - evidence on progress and recommendations for cooperative actions - Final European progress report*, European Commission,

*DG Information Society and Media, ICT for Health Unit*. Available at: [http://www.ehealthnews.eu/images/stories/pdf/ehstrategies\\_final\\_report.pdf](http://www.ehealthnews.eu/images/stories/pdf/ehstrategies_final_report.pdf) (Accessed: 28 June 2017).

Subramanian, N. and Jeyaraj, A. (2018) 'Recent security challenges in cloud computing', *Computers & Electrical Engineering*. Pergamon, 71, pp. 28–42. doi: 10.1016/J.COMPELECENG.2018.06.006.

Thilakanathan, D. (2016) *Secure Data Sharing and Collaboration in the Cloud*. The University of Sydney. Available at: <https://sydney.edu.au/engineering/electrical/about/UserFiles/File/THILAKANATHAN.pdf> (Accessed: 29 June 2017).

Thorp, J. *et al.* (2015) *Report on the use of cloud computing in health*. D7.2.1. Available at: <http://grants.nih.gov/grants/guide/notice-files/NOT-OD-15-086.html> (Accessed: 15 July 2019).

Veeramachaneni, V. K. (2015) 'Security Issues and Countermeasures in Cloud Computing Environment', *International Journal of Engineering Science and Innovative Technology (IJESIT)*, 4(5), pp. 82–93. Available at: [http://www.ijesit.com/Volume 4/Issue 5/IJESIT201505\\_10.pdf](http://www.ijesit.com/Volume%204/Issue%205/IJESIT201505_10.pdf) (Accessed: 5 March 2019).

Vinegar, D. (2013) 'The rise and fall of telehealth in 2013 | Healthcare Professionals Network | The Guardian', *Healthcare Network*, 3 December. Available at: <https://www.theguardian.com/healthcare-network/2013/dec/03/nhs-telehealth-rise-and-fall> (Accessed: 30 June 2017).

Ward, B. T. and Sipior, J. C. (2010) 'The Internet Jurisdiction Risk of Cloud Computing', *Information Systems Management*. Taylor & Francis Group , 27(4), 249

pp. 334–339. doi: 10.1080/10580530.2010.514248.

Watson, R. (2010) 'European Union leads way on e-health, but obstacles remain.', *BMJ (Clinical research ed.)*. BMJ, p. c5195. doi: 10.1136/bmj.c5195.

Webster, J. and Watson, R. T. (2002) 'Analyzing the past to prepare for the future: writing a literature review', *MIS Quarterly*. Society for Information Management and The Management Information Systems Research Center, 26(2), pp. xiii–xxiii. Available at: <https://dl.acm.org/citation.cfm?id=2017162>.

Whaiduzzaman, M. *et al.* (2014) 'A survey on vehicular cloud computing', *Journal of Network and Computer Applications*, 40, pp. 325–344. doi: 10.1016/j.jnca.2013.08.004.

Whitten, P. and Kuwahara, E. (2004) 'A multi-phase telepsychiatry programme in Michigan: organizational factors affecting utilization and user perceptions.', *Journal of telemedicine and telecare*, 10(5), pp. 254–61. doi: 10.1258/1357633042026378.

Williams, M. E., Ricketts, T. C. and Thompson, B. G. (1995) 'Telemedicine and Geriatrics: Back to the Future', *Journal of the American Geriatrics Society*. Blackwell Publishing Ltd, 43(9), pp. 1047–1051. doi: 10.1111/j.1532-5415.1995.tb05572.x.

Youssef, A. and Youssef, A. E. (2014) 'A Framework for Secure Healthcare Systems Based on Big Data Analytics in Mobile Cloud Computing Environments', *International Journal of Ambient Systems and Applications (IJASA)*, 2(2). doi: 10.5121/ijasa.2014.2201.

Zanaboni, P. and Wootton, R. (2012) 'Adoption of telemedicine: from pilot stage

to routine delivery', *BMC Medical Informatics and Decision Making*, 12(1), p. 1.  
doi: 10.1186/1472-6947-12-1.

Zhang, R. and Liu, L. (2010) 'Security Models and Requirements for Healthcare Application Clouds', in *3rd IEEE International Conference on Cloud Computing (CLOUD '10)*, pp. 268–275. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.165.7184&rep=rep1&type=pdf> (Accessed: 2 July 2019).

Zissis, D. and Lekkas, D. (2012) 'Future Generation Computer Systems Addressing cloud computing security issues', *Future Generation Computer Systems*, 28, pp. 583–592. doi: 10.1016/j.future.2010.12.006.

## **List of Publications**

- ⇒ Factors limiting the adoption of Cloud Computing in Teleradiology, 10-13 December 2018, 13th International Conference for Internet Technology and Secured Transactions (ICITST-2018), University of Cambridge, UK.
- ⇒ Extended version accepted and published in International Journal for Information Security Research (IJISR), Volume 9, Issue 1, IISSN 2042-4639(Online).
- ⇒ Current Cybersecurity Maturity Models: How Effective in Healthcare Clouds, accepted and presented at the Collaborative European Research Conference (CERC 2019), University of Applied Sciences, Darmstadt, Germany. CERC Workshop Proceedings, Vol-2348, ISSN 1613-0073
- ⇒ Maturity Model for Healthcare Cloud Security, Information and Computer Security journal (Emerald Publishing).